RICE UNIVERSITY

Design and Evaluation of Primitives for Passive Link Assessment and Route Selection in Static Wireless Networks

by

Stanislav Miskovic

A Thesis Submitted
in Partial Fulfillment of the
Requirements for the Degree

Doctor of Philosophy

Approved, Thesis Committee:

Edward W. Knightly, Chair
Professor of Electrical and Computer Engineering and Computer Science

David B. Johnson
Professor of Computer Science

Ashutosh Sabharwal
Associate Professor of Electrical and Computer Engineering

Houston, Texas

April, 2012

ABSTRACT

Design and Evaluation of Primitives for

Passive Link Assessment and Route Selection

in Static Wireless Networks

by

Stanislav Miskovic

Communication in wireless networks elementally comprises of packet exchanges over individual wireless links and routes formed by these links. To this end, two problems are fundamental: assessment of link quality and identification of the least-cost (optimal) routes. However, little is known about achieving these goals without incurring additional overhead to IEEE 802.11 networks. In this thesis, I design and experimentally evaluate two frameworks that enable individual 802.11 nodes to characterize their wireless links and routes by employing only local and passively collected information.

First, I enable 802.11 nodes to assess their links by characterizing packet delivery failures and failure causes. The key problem is that nodes cannot individually observe many factors that affect the packet delivery at both ends of their links and in both

directions of 802.11 communication. To this end, instead of relying on the assistance of other nodes, I design the first practical framework that extrapolates the missing information locally from the nodes' overhearing, the observable causal relationships of 802.11 operation and characterization of the corrupted and undecodable packets. The proposed framework employs only packet-level information generally reported by commodity 802.11 wireless cards.

Next, I design and evaluate routing primitives that enable individual nodes to suppress their poor route selections. I refer to a route selection as poor whenever the employed routing protocol fails to establish the existing least-cost path according to an employed routing metric. This thesis shows that an entire family of the state-of-the art on-demand distance-vector routing protocols, including the standards-proposed protocol for IEEE 802.11s mesh networks, suffers from frequent and long-term poor selections having arbitrary path costs. Consequently, such selections generally induce severe throughput degradations for network users. To address this problem, I design mechanisms that identify optimal paths locally by employing only the information readily available to the affected nodes. The proposed mechanisms largely suppress occurrence of inferior routes. Even when such routes are selected their durations are reduced by several orders of magnitude, often to sub-second time scales.

My work has implications on several key areas of wireless networking: It removes systematic failures from wireless routing and serves as a source of information for a wide range of protocols including the protocols for network management and diagnostics.

To my mother.

Acknowledgments

Graduate research is a unique experience of advancing knowledge and embarking on a profound personal journey. Blissful discoveries shed light on persistent hardships. I was fortunate to share both with an extraordinary group people, my friends.

I am deeply grateful to my advisor Prof. Edward W. Knightly who provided me with an opportunity to study at Rice University. His enthusiasm motivated me, his patience gave freedom to my research, his strong orientation towards conceptual thinking improved my work immensely.

I also extend my gratitude to Prof. David B. Johnson and Prof. Ashutosh Sabharwal who served as my thesis committee members, and much more: Prof. Sabharwal provided me with his exuberant assistance in search for my career directions. For that I have no words to thank him enough. Prof. Johnson made my thesis presentations unique and interesting as a true intellectual discussion should be: challenging, friendly and insightful.

Most of my work would not have been possible without the wireless network that serves a low-income neighborhood in Houston, TX. Efforts of Jim Forrest, Will Reed and other people from the Technology For All organization assisted me in serving those of us who have less means in our lives. This gave meaning to my research.

I owe the endurance in my graduate work to friendship with extraordinary people from our research group: Eugenio, Ryan, Tasos, Ahmed, Ehsan, Bruno, Oscar, Naren, Joshua, Joe, Omer, Jingpu and our new rising star Adriana.

And then, there are Eugenio Magistretti and Natalia Castro, what a wonderful pair of people. When I was happy we laughed together, when hardships were overwhelming they were there for me. Their kindness had no end.

St. Sava Serbian Orthodox Church in Houston, TX will always have a special place in my heart. When work was becoming all my world, it was a window to life and meaning. I owe special gratitude to Fr. Dejan Tiosavljevic and Jonathan Stigant for their exemplary guidance in being a better, kinder and more humble person. Nada Kovacevic, Ljuba Janjic, Mylan and Kathy Radulovich made me feel as if I never left home. Nedeljko Visekruna has always put a smile on my face with his own special views on philosophy.

I dedicate this thesis to my mother Vera, to her loving care and support: Mom, I thank you for everything I have achieved and for all care-free moments in my life. To my father Mihailo and his unceasing faith in me, I owe an endless gratitude. I wish my grandparents Teodor and Milica were still here with us to share their happiness with me.

Finally, I praise the Lord for His blessings and keeping hope and joy in my heart.

Contents

Illustrations

Tables

Chapter 1

Introduction

Wireless networks based on IEEE 802.11 standards have evolved from isolated deployments to an almost ubiquitous communication service in which nodes increasingly contend and interfere with each other. These interactions together with the time-varying properties of wireless channels affect communication quality, thus requiring timely characterization as well as identification of the best available communication resources. In this thesis, I address these two fundamental networking problems: I design and experimentally evaluate methodologies that characterize causes and properties of packet losses at wireless links, and suppress selection of non-least-cost paths in IEEE 802.11 networks.

Effective acquisition of measures that indicate link and path quality is critical for achieving the above objectives. Specifically, while the optimal (least-cost) paths can be identified by frequently exchanging routing updates [1, 2, 3], and wireless links can be characterized by employing distributed network measurements [4, 5, 6, 7, 8, 9, 10], such approaches can be prohibitively intrusive to ongoing communications [11]. Hence, wireless networking has reached a crossroads: The designs that rely on a network-wide overhead are known and can provide accurate results, but there is a growing need for less disruptive approaches. I devise methods that employ only the passively collected information at individual nodes in order to improve the nodes' routing decisions and packet loss evaluations. The performance of such methods is largely unknown in the existing research.

Passive and Local Link Assessments

Link assessments identify and characterize factors that affect direct communication between pairs of nodes. I focus on the factors that induce packet losses to ongoing communications, showing that individual nodes can characterize these factors while acting independently. The key problem is that the nodes can only observe a subset of packet-loss causes and occurrences, which lead researchers to an understanding that local observations are insufficient for link assessment. For example, a sending node cannot directly identify whether its packet deliveries fail due to channel conditions or packet collisions at the receiving end of its link. Similarly, without decoding the senders' addresses, receivers cannot directly associate the corresponding losses to any links. Therefore, to obtain targeted assessments of link quality, I develop methods that extrapolate the missing assessment information.

I show that such extrapolation is achievable with the assistance of indications provided by undecodable or corrupted packets as well as a rich set of causal relationships embedded in the IEEE 802.11 MAC protocol. For example, one such relationship enables senders to identify packet capture occurrences at their receivers: Based on the premise that capture winners shorten their backoff, the proposed sender-side methods reconstruct capture relationships by analyzing the rates of overheard ACK feedback.

To understand the timescales and accuracy of such reconstruction, I calibrate assessment indications via experiments in controlled wireless environments.

Passive Identification of Optimal Routes

Identification of optimal paths is a fundamental routing functionality which enables nodes to learn about their least-cost paths according to an employed routing metric. In this thesis, I address the underlying mechanisms that enable such identification for a wide range of the state-of-the-art wireless routing protocols based on the on-demand route discovery and distance-vector identification of path costs [12, 13, 14, 15]. Moreover, I develop a set of new mechanisms that suppress non-least-cost route selections.

Conducting the first systematic analysis of route selection primitives, I show that the addressed family of routing protocols inherently yields inferior route selections. Given that such primitives perform on-demand route discovery for pairs of nodes, I refer to them node-pair routing primitives. I localize the problem of poor route selection to the overhead reduction actions and show that they are overly restrictive and distribute insufficient routing information. Consequently, only a subset of nodes is informed about their optimal paths, while such paths are effectively hidden for many other nodes in each discovery. My extensive measurements in a large residential wireless mesh network show that inferior route selections occur regularly and cause long-term throughput degradations for network users.

The key question is how to recover the missing information about least-cost paths without reverting to overhead-intensive routing [1, 2, 3]. To this end, I develop a principle of historical path ranking. The ranking identifies unreported feasible paths candidates for optimal route selection by employing only the local and readily available information reported to a node in previous route discoveries. To identify whether this historic information can indicate presently best paths, I perform extensive experimental evaluation and show that this is the case. Based on this finding, I devise routing primitives that locally suppress inferior route selections and restore optimal paths. The restoration is based on informed local requests for present costs of path candidates inferred as historically best. Employing only present path costs, the proposed routing framework avoids the problem of route selections based on stale information inherent to existing route caching mechanisms [16].

1.1 Summary of Thesis Contributions

Link assessment and selection of optimal (least-cost) routes address two fundamental problems of wireless networking. This thesis makes following contributions:

- *Near real-time link characterization.*

  While the existing approaches to link assessment address incomplete assessment insights of individual nodes by waiting for assessment reports of other nodes or network management entities, this thesis introduces the first practical framework for link assessment by individual nodes: The proposed approach is timely and achieves near real-time assessment updating at the rate of aggregate overheard traffic. I show that such updating approaches time scales of per-packet transmissions in a large operational network.

- *Assessments reflecting actual communication conditions.*

  Another unique advantage of the proposed link assessment framework is that it derives results from the actual network traffic, thus being inherently representative of the actual communication conditions at the assessed links. Instead, the existing approaches generally extract their assessments from probes sent at specific rates, modulation types and packet lengths. Such link assessments produce results that are generally representative only of the communication conditions for the employed set probing parameters.

- *Augmentation of partially available assessment information.*

  The fact that individual nodes can only partially observe factors that affect their packet delivery has lead to development of link assessment frameworks that require assistance of other nodes, i.e., the external sources of missing information. These frameworks often require that a node belong to a specific administrative domain or that it employ additional protocols for exchange of assessment measurements. Instead, this thesis shows that individual nodes can independently assess their links in any statically deployed IEEE 802.11 setting, including the "networks" formed by the unintended collocations of 802.11 nodes. I show that the missing assessment knowledge of individual nodes can be extrapolated from locally measurable causal relationships inherent to 802.11 protocol operation, as well as the auxiliary indications provided by the corrupted and undecodable packets.

- *The first systematic analysis of on-demand distance-vector routing.*

  While the problem of inferior route selection has been observed in simulation studies [17, 18] and in operational networks [19], the origins of such selections were not characterized before this thesis. This work explains systematic origins of inferior route selections originating from the standardized and widely-deployed mechanisms shared by an entire family of wireless routing protocols. One such protocol is proposed by the IEEE 802.11s standard for wireless mesh networks [20]. I show that such mechanisms yield inferior route selections irrespective of the employed routing protocols, routing metrics, or losses of route discovery information.

- *Characterization of the systematically induced inferior route selections.*

  The thesis shows that systematically-induced inferior route selections result from the effective hiding of least-cost paths, thus deceiving a subset of nodes to selection of their suboptimal (non-least-cost) routes. These nodes then falsely perceive such selections as the optimal ones, thus maintaining the poor routes. My experiments in a large wireless mesh network show that such routing conditions cause long-term throughput degradations for network users. On the other hand, this result is similarly important for wireless service providers: The providers' investments in wireless infrastructure may be futile, because the best available network resources may remain "hidden" due to the actions of the state-of-the-art routing protocols.

- *Identification of optimal paths enabled by historic persistence of network properties.*

  This thesis explains and experimentally shows how to identify the missing information about the least-cost paths by ranking path costs reported in previous route discoveries. Despite wireless networks having many variable properties, such as radio propagation and traffic load, I show that a number of key properties are largely historically persistent. This enables employment of historic information in present path-selection decisions. Moreover, such approach does not induce any additional traffic overhead, thus not being disruptive to any ongoing communications. Applying the devised methods of historically-assisted routing, I show that selection of inferior paths is largely suppressed or reduced to sub-second timescales.

1.2 Thesis Overview

The thesis proceeds as follows. In Chapter 2, I introduce and develop PaL, a system for wireless link assessment based on passively collected information and local decisions of individual nodes in IEEE 802.11 networks. I further explain PaL's implementation in Linux kernel and perform extensive evaluation in the network with real users as well as in a setting with controlled and repeatable experimental conditions.

In Chapter 3, I propose a wireless routing redux: I identify systematic failures in on-demand distance-vector routing and show the extent of consequent problems by experiments in our wireless mesh network serving a large residential area of about 4 km^2. The chapter also introduces design and evaluation of new historically-assisted routing primitives. In Chapter 4, related work is discussed on both topics addressed in this thesis. Finally, in Chapter 5, I conclude by discussing implications and future directions of the presented research.

Chapter 2

PaL: A System for Passive and Local Link Assessment in Wireless Networks

2.1 Introduction

Communication in wireless networks elementally comprises of packet exchanges over individual wireless links. As some packet exchanges inevitably fail, assessment of the causes and likelihood of *failures* of such packet exchanges is valuable for numerous networking functions including network diagnostics and management, rate adaptation, and route selection. An accurate assessment must incorporate that link quality can be affected by many factors including MAC-layer link interactions, channel conditions and settings of IEEE 802.11 protocol parameters. Existing approaches to link assessment employ probing and reporting, thus decreasing throughput of other flows via increased interference, MAC-layer contention and decreased available air time. Consequently, probing and reporting rates must be limited, but such limits also constrain the rate at which link assessments can be updated.

This thesis proposes and evaluates PaL, a link assessment methodology that is non-disruptive to on-going traffic, provides assessment updates at the rate of the actual traffic, and is representative of the link's quality for actual data communications. To this end, PaL enables each node to assess its links *passively* and *locally* by employing packet-level information provided by commodity IEEE 802.11 wireless cards. Specifically, each node assesses its links independently by relying only on its own transmissions, receptions and any overheard traffic. The key challenge for this technique is the inability of individual nodes to directly measure events affecting both ends of the link and both directions of IEEE 802.11 packet exchange over the link. Consequently, I present following contributions.

First, PaL's assessments address: *(i) Bi-directional link assessment in the presence of asymmetry.* A node measures different parameters depending on whether it acts as a transmitter or receiver, yielding measurement asymmetry. Moreover, a node's assessments are exposed to communication asymmetry due to interactions of link's endpoints with different sets of neighbors and hidden terminals. *(ii) Incomplete information.* Commodity 802.11 devices report a limited set of communication parameters while packet loss, corruption, and "deafness" during transmissions further limit measurement data. I develop assessment methods that rely on extrapolation of available assessment measures and results of offline channel-emulator-based training to counter these two assessment problems during PaL's real time operation. The proposed methods augment passive measurements by employing information about the undecodable delivery failures reported by common 802.11 devices (but ignored by existing link-assessment approaches), as well as information from inherent 802.11 ACK feedback at each link. Moreover, the assessment extrapolation is based on causal relationships inherent to 802.11 operation.

Second, I perform assessment experiments in an operational network and a controlled experimental environment. In the operational network, because PaL's assessments are updated passively via ongoing traffic, all of a node's incoming and outgoing links can be fully characterized in intervals of about 2 ms. By utilizing and extrapolating from a large number of observation events (vs. only a single link to be assessed at a time), nodes characterize the quality of their links for a broad set of the actual modulation rates, packet sizes and SNRs at the updating rates that are unparalleled by active approaches to link assessment. To achieve similar updating rates, active assessment would have to severely disrupt network operation. I show that operational networks commonly encounter multiple sources of asymmetry and limited assessment information. Specifically, while evaluating a link in a large wireless network of a university department, more than 20 hidden terminals of each endpoint node were identified attributing to communication asymmetry. Also, my results indicate that the link's receiver was able to fully characterize just 30% of the sender's failed packet deliveries by decoding them and being able to recover the sender's address. To systematically analyze the factors of asymmetry and incomplete information, I extended PaL's evaluation to employ an Azimuth channel emulator.* The evaluation shows that these factors are exacerbated with increased rates of collisions at which assessing nodes become increasingly deaf to events occurring at the link. Consequently, while a node can assess that a link is poor due to increased packet losses, its ability to identify the causes of loss diminishes with load.Fortunately, the obtained results also indicate that operational networks rarely operate in the state of high collision rates.

*Azimuth ACE 400 WB, http://www.azimuth.com

Third, I conduct controlled experiments to evaluate assessment accuracy and provide PaL's offline training via a channel emulator. I first address PaL's methods that do not require training and show that senders can accurately extrapolate information about the causes of their failed packet deliveries at receivers, even though such causes cannot be directly observed. Employing retransmission distributions, the senders can continually identify whether their deliveries fail predominantly due to channel conditions or collisions at the receiver. Moreover, PaL enables senders to reconstruct packet capture relationships at their receivers by analyzing ACK feedback properties in approximately 300 ms intervals. Other PaL methods for reconstruction of hidden terminal activity and actual rates of losses employ offline training. I show that such training is easily feasible in practice enabling the link's endpoints to exploit a wealth of predictable relationships between measurable parameters and the actual factors that affect the link's packet delivery. For example, the obtained results indicate that accurate calibration of sender-side assessments of hidden terminal activity can be achieved by overhearing just 20% of hidden terminal ACKs. Similarly, receivers can extrapolate their assessments of uncharacterized packet losses by anchoring their estimation on decodable delivery failures.

This work has key implications for a wide range of protocols including modulation and coding rate adaptation and routing. For example, routing protocols require a “cost” for each link [21, 22] and rate adaptation protocols can be enhanced with a timely representation of the reasons for loss, i.e., if due to fading or hidden terminals [23, 24, 25]. Moreover, PaL's results provide important insights to network management and diagnostic tools.

The remainder of this chapter is organized as follows: Sections 2.2, 2.3, 2.4, 2.5 present PaL's core components including transmitter identification and sender and receiver side assessment. The remaining sections present the evaluation platforms and experimental validation.

2.2 Scope of PaL Assessments

In this section, I introduce the scope and goals of PaL's assessments and constraints imposed by passive and local acquisition of assessment information.

2.2.1 System Model

I address *passive* characterization of the quality of wireless links in IEEE 802.11 wireless networks and estimate the *causes* and *properties* of their DATA[†] delivery failures. Specifically, I focus on failures affected by channel conditions, uncoordinated 802.11 transmissions and packet capture effects.

I consider a node A assessing its links transmitting outbound data $L(A, n_i)$ and links receiving inbound data $L(n_i, A)$. As packet delivery failures in two link directions can be quite different, separate assessments are devised for each direction. The links share a common IEEE 802.11 radio channel with an *a priori* unknown number other nodes (see Figure 2.2.1). The key property of PaL is that links are continually characterized based on any exchanged or overheard packets.

The assessing node A employs no collaboration with other nodes in the network towards achieving its assessments, thus precluding probing neighbors or querying neighbors for extraneous assessment information. Instead, the node collects all assessment data *passively* via packet-level reports provided by its commodity 802.11 device employed in communications and traffic overhearing. Specifically, PaL's as-

[†]DATA denotes packets carrying communication payload in IEEE 802.11 DATA-ACK packet exchange.

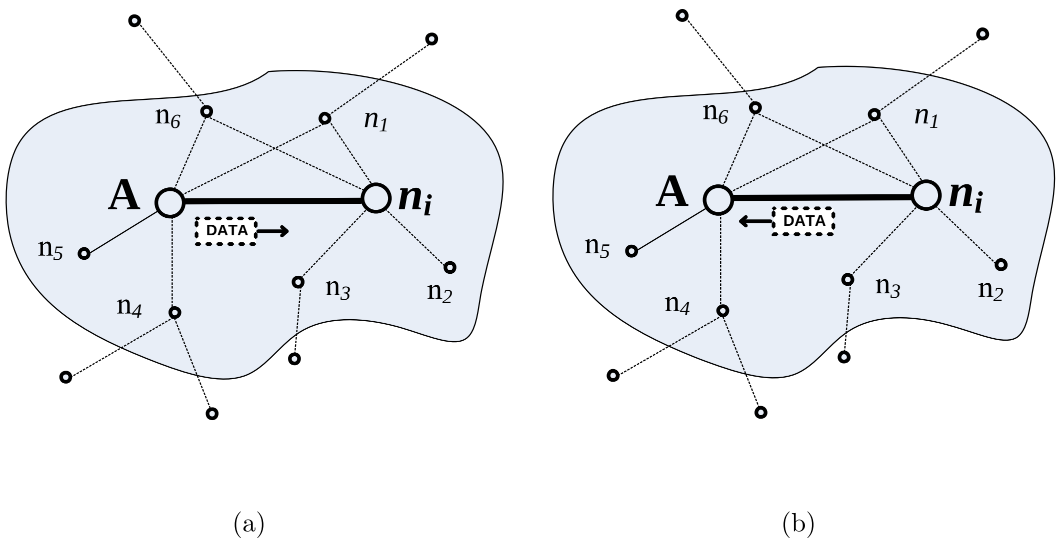


Figure 2.1 : Node A assessing its link in (a) outbound and (b) inbound DATA directions.

sessments are based on the node's packet transmissions, packet receptions and any overhearing that can be decoded or only detected. Given this system model, PaL can operate in general network settings, spanning both "randomly" formed networks, such as overlapping residential deployments or hotspots of different businesses, as well as planned networks such as enterprise WLANs or urban mesh networks.

2.2.2 Taxonomy of Assessment Problems

The key assessment problem is that local and passively collected information does not directly capture important factors that affect packet delivery failures in either direction of the link. I address two key issues: *(i)* partial availability of assessment measures and *(ii)* assessment asymmetry.

Partial Availability of Assessment Measures represents a permanent or transient lack of data that would otherwise directly indicate specific events leading to packet delivery failures. In PaL, this is due to a limited set of communication parameters reported by commodity IEEE 802.11 devices, as well as communication effects that preclude packet reception and overhearing.

PaL's input measurements are restricted to packet-level parameters reported by commodity 802.11 devices. While these parameters enable PaL to identify a rich set of assessments, such as packet airtime, packet error rate or link's SNR, many aspects of failed DATA deliveries remain hidden. For example, both DATA transmitter and receiver have a limited insight into retransmission events which I will show are a key factor for assessing the causes of packet delivery failures.

Next, communication effects of transmission deafness and collisions may preclude the assessing nodes from obtaining some or all of the parameters exported by 802.11 devices. As illustrated in Figure 2.2, the number of reported parameters depends on packet reception and overhearing properties: The packet may not even be detected; only its SNR would be reported after the reception of PLCP preamble, its modulation rate after the reception of PLCP header, and the rest of the listed parameters may be reconstructed after the reception of MAC header. To this end, PaL is the first link assessment framework that operates under such heterogenous availability of assessment data.

Assessment Asymmetry represents a state in which different nodes have inconsistent views of factors that affect packet exchange. Such asymmetry occurs both in measurements and in communication patterns. Measurement asymmetry reflects the

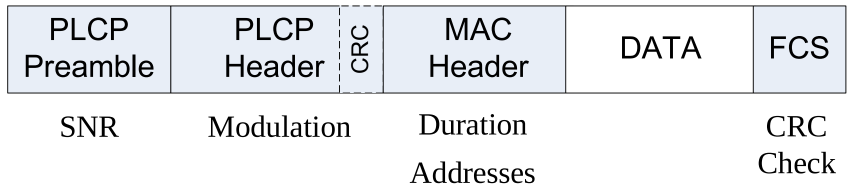


Figure 2.2 : Assessment components within a packet.

fact that transmitters and receivers observe different sets of communication parameters, while communication asymmetry occurs due to different interactions of link's endpoints with different sets of neighbors and hidden terminals. Consequently, transmitters have no direct indications of events that occur at the receiving end of the link, thus being *a priori* oblivious to the causes of failed DATA deliveries. On the other hand, receives would only identify that delivery failed at a specific link by decoding the packets and reconstructing the packet's transmitter identities. Given that many packet transmissions may not be decodable, receivers can perceive only a subset of failed deliveries while senders have a complete information about the outcomes of all their delivery failures via ACK feedback. Due to the described asymmetries, I develop separate methods for inbound and outbound links for which the assessing node acts as data receiver or transmitter.

2.2.3 Assessment Methodology

Given that the raw data used for assessment is inherently incomplete, PaL's overarching objective is to extrapolate this data to estimates of causes and properties of packet losses. To this end, the first step is to identify at which inbound links the failures occur and which hidden terminals induce packet losses at outbound links. Both of these problems are addressed by the methods for identification of transmitters. Next, PaL employs this underlying information and develops separate methods for inbound and outbound links. These methods characterize packet-loss properties, such as the traffic rate of collision-inducing transmitters, by exploring various causal relationships inherent to IEEE 802.11 MAC operation or by leveraging reference calibrations established in the representative controlled environments.

2.3 Identification and Profiling of Transmitters

To assess wireless links, PaL must first identify transmitting nodes for all information it receives or overhears. For inbound links, such identification is necessary because failed packet deliveries contain bit-errors (at best) and can only be attributed to specific links after PaL reconstructs sender identities from such errors. Moreover, transmitter identification enables PaL to identify collision-inducing nodes that affect links. For outbound links, PaL's identification methods enable partial reconstruction of the node's two-hop neighborhood and hidden-terminal relationships in that neighborhood.

2.3.1 Restoration of Transmitter Identities

PaL restores sender identities from decodable packets that contain bit-errors indicated by the IEEE 802.11 FCS checksum. For inbound links, these packets are PaL's only source of information that fully characterizes failed deliveries, indicating modulation rates, payload sizes and corresponding SNRs.

Restoration is partially based on *minimal Hamming distance of decoded MAC addresses*: I consider previously identified correct addresses of transmitters as anchoring points in the MAC address space. Then, for each corrupted packet, PaL reconstructs the address of a sender to the Hamming-closest correct address. The correctness and reconstruction capabilities of this method depend on Hamming half-distances between correct addresses: The larger the distance, the more corrupted bits can be successfully restored. I refer to such distances as correction range and illustrate them in Figure 2.3. To this end, the assumption is that MAC addresses in operational settings are sufficiently separated, with potential exceptions when infrastructure nodes originate from similar production series and have mostly consecutive addresses. Such nodes may be present in enterprise WLAN backhauls or urban mesh networks.

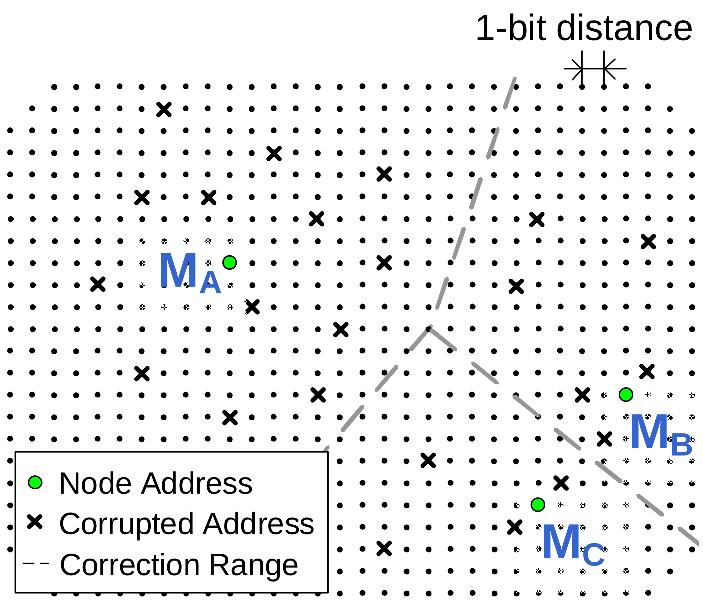


Figure 2.3 : Hamming reconstruction of transmitter identities.

To augment restoration of transmitter identities and characterize channel conditions of links to each transmitting node, PaL employs *per-transmitter SNR profiling*. The profiling serves as a tiebreaker in cases of “corrupted” addresses being Hamming-equidistant from multiple candidate senders, i.e., being at the boundaries of correction ranges. Namely, PaL establishes SNR profiles by continually overhearing packet transmissions of nodes and by measuring their corresponding SNRs. The profile of each node consists of an EWMA value and standard deviation of corresponding SNR measurements. Based on such profiles, PaL attributes a corrupted packet transmission to a candidate sender with "closer" average SNR to the measured SNR of the corrupted packet. If SNR profiles of candidate senders overlap, PaL does not make any assignment.

2.3.2 Identification of Collision Sources

PaL enables both link endpoints to partially reconstruct their 2-hop neighborhoods. The key to this reconstruction is identification of the link's collision sources. To this end, I identify these sources via ACK feedback, decoding of near noise-floor packets and interpretation of IEEE 802.11 protocol rules that indicate uncoordinated transmissions.

Identification via overheard ACK feedback enables senders to identify their collision sources at outbound links. Overhearing ACKs and never overhearing corresponding DATA identifies the ACK's destination as a hidden terminal. Figure 2.4(a) illustrates an example for the assessing node S_A and its hidden terminals h_1 and h_2. Although simple, this method is highly effective in identifying existence and activity of hidden terminals even when they change their communication patterns. A hidden terminal can be continually characterized as long as it communicates with any of the transmitter's neighbors, such as neighbors n_1 and n_2 in Figure 2.4(a).

Second, I employ *decoding of near noise-floor packets* to identify collision sources at outbound links that may not be communicating with any neighbors of the assessing node (see Figure 2.4(b)). While such identification is theoretically infeasible

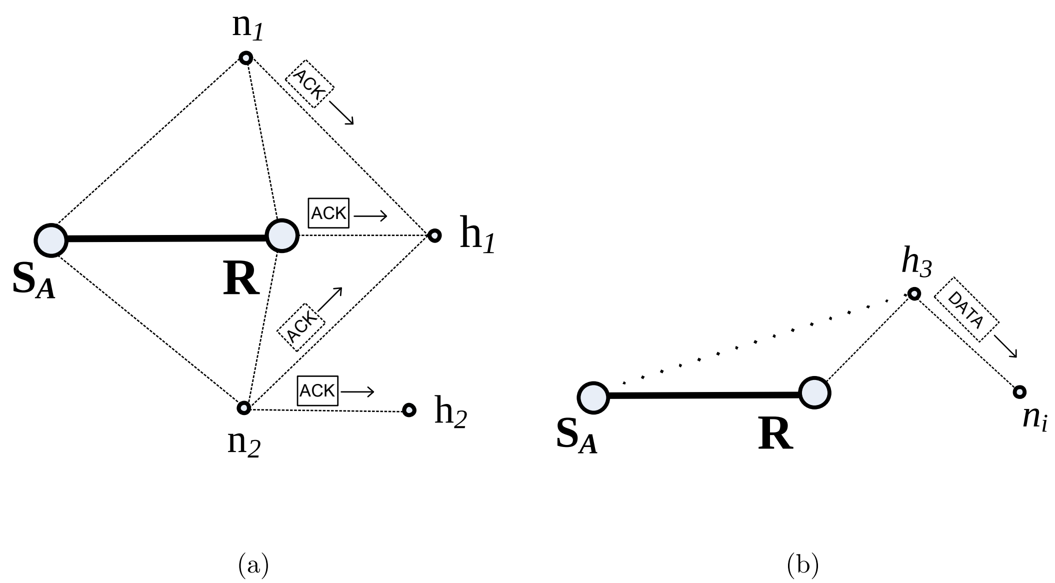


Figure 2.4 : Identification of collision sources at outbound links: (a) ACK overhearing and (b) near noise-floor packet decoding.

because any packet detection should induce backoff and coordinate transmissions of two nodes, in practice this is not the case. First, common mechanisms of automatic gain control [26, 27] characterize packets overheard at near noise-floor levels as interference and avoid backing off to them. Second, while the IEEE 802.11 standard mandates packet reception sensitivity of $-75\ dBm$ to $-82\ dBm$ depending on the modulation rate, I will show that commodity 802.11 devices have much higher sensitivities. Therefore, the assessing node S_A can overhear its collision source h_1 without backing off to it.

PaL's *Packet Collision Processing* enables link endpoints to identify each others' collision sources. At outbound links, such sources are identified by overhearing any packets during the intervals of expected ACK arrivals over the link. At inbound links, the sources of collisions are identified in a subset of packet captures that reveal both colliding packets as decodable. Moreover, even when a colliding packet cannot be decoded, collisions can be identified by detecting packets within DIFS intervals following previous packet receptions. In this way, this work is the first to show that individual nodes can independently process collision events at both ends of their links.

2.4 Outbound Link Assessments

The key problem of outbound link assessments is that failures in DATA delivery occur at the other end of the link, such that failure causes cannot be directly identified. The goal of PaL's methods is to characterize these causes. I develop methods that extrapolate the missing information from retransmission distributions and ACK feedback, as well as by employing calibration established by offline training.

2.4.1 Classification of Failure Causes Based on Retransmission Distributions

Without any direct measures to indicate causes of delivery failures for outgoing DATA, I base the outbound link assessment on analysis of per-packet retransmissions, i.e., a histogram of the number of retries required for each new packet transmission. In particular, PaL continuously monitors a link's retransmission distribution hypothesizing that the distribution differs according to whether the link is dominated by channel-induced vs. collision-induced losses. Namely, channel-induced losses are time-varying due to fluctuating channel conditions and can be suppressed by various receiver mechanisms such as automatic gain control, active interference avoidance or modulation rate adaptation. In contrast, collisions are induced by topological factors (hidden terminals) that are more persistent than channel conditions in statically deployed wireless networks that I address in this thesis. This disparity in capabilities of addressing the two causes of losses motivates the proposed assessment method.

To enable a practical implementation, I characterize retransmission distributions by observations of histograms $H^{(i)}, i \in N$ in consecutive time slot intervals T_H. Such characterization enables PaL to produce timely assessments after each time slot. To identify a specific packet loss environment, I establish the corresponding reference histograms $\{H^R\}$ from the results of offline training in representative controlled environments dominated by channel fading, collisions or their joint presence. To account for the randomness in fixed-time measurements, each histogram bin $h_k^R \subset H^R, k \in \{0, maxRetry\}$ has confidence intervals also established by offline training. Then, I determine the thresholds at histogram bins that indicate each environment. PaL uses these thresholds during its real-time operation to continually estimate the dominant causes of packet losses in operational networks by estimating the likelihoods that the measured histogram values indicate each cause.

2.4.2 Identification of Hidden Transmitter Traffic Rates

Next, I address sender-side characterization of its DATA collisions occurring at the receiver. The key parameter to be estimated is the rate of collision-inducing traffic, i.e., the traffic rate of hidden transmitters. I develop two assessment methods depending on the sender's ability to identify individual hidden nodes.

Blind Identification. First, when collision sources cannot be identified individually, i.e., the ACKs sent to them cannot be overheard, as shown in Figure 2.5(a), PaL infers the aggregate rate of colliding traffic. To this end, I employ the sender's complete knowledge of three key parameters: the rates of its transmissions and failed packet deliveries, and an estimate of changes in the link's channel conditions. The hypothesis is that for a given set of communication parameters the causes of failed packet deliveries can be separated, such that the extent of loss rate due to channel conditions can be identified, while other losses can be attributed to collisions. PaL identifies the link's channel condition via *SNR profiling* obtained by the measurements of packets arriving from the link's receiver. For the identified channel condition, I determine the reference loss rates by off-line training in representative controlled environments. Likewise, the training establishes a relationship between measured loss rates and the actual aggregate traffic rate of hidden terminals. Consequently, we can extrapolate PaL's loss rate measurements to an aggregate hidden-terminal traffic rate.

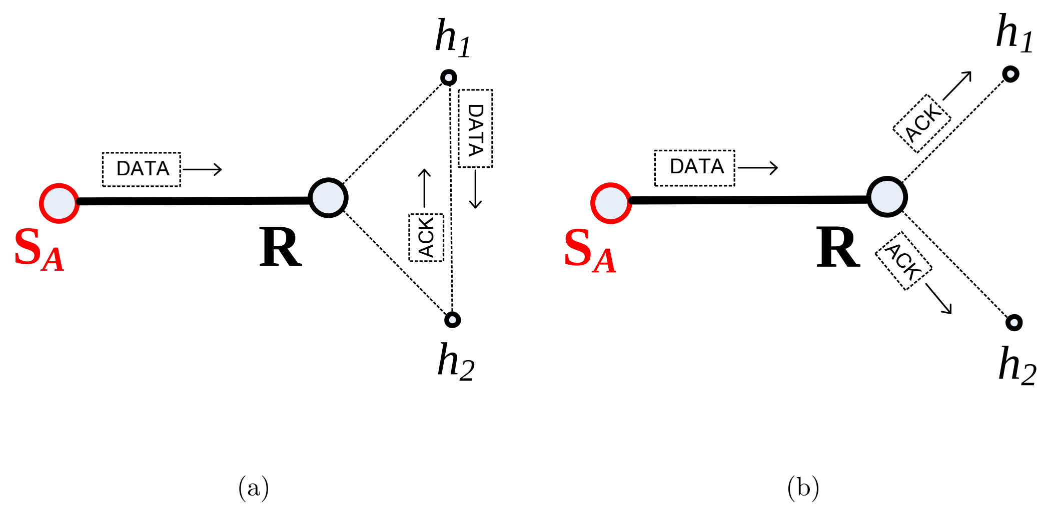


Figure 2.5 : Sender's S_A identification of hidden terminal activity: (a) Blind identification, and (b) Identification by ACK analysis.

Identification via ACK Feedback Analysis. Next, when collision sources can be individually identified via PaL's identification methods, I estimate each sender's individual transmission rate by overhearing their ACK feedback, as shown in Figure 2.5(b). Although such characterization is more informed, the rate inference is not immediate: The key problem is that ACK feedback is a sparse representation of hidden terminal activity, because it only indicates the successful packet deliveries. Moreover, many ACKs may not even be overheard due to the assessing sender's transmission deafness. For example, deafness for a single hidden terminal h_1 at the assessing sender S_A is illustrated in Figure 2.6.

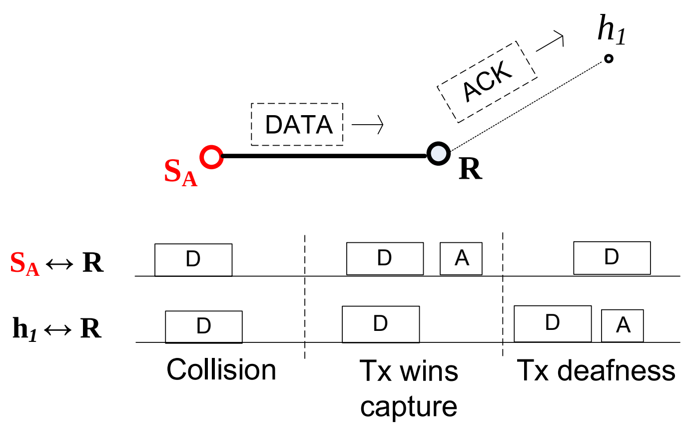


Figure 2.6 : ACK-feedback sparsity: Events in which the assessing sender S_A cannot overhear any ACKs related to activity of its hidden terminal h_1.

Deafness occurs when S_A transmits a packet and loses capture at the receiver R: Being still in transmission mode, the sender S_A will be deaf to the ACK subsequently sent from the receiver R to the hidden terminal h_1. My hypothesis is that the rate of overheard ACKs is related to the actual transmission activity of the hidden terminal, and that these relationships can be identified knowing the three key parameters employed in PaL's blind identification. Specifically, for reconstruction I employ a causal relationship of the IEEE 802.11 MAC operation: Fewer overheard ACKs indicate more collisions and larger 802.11 backoffs which reduce the hidden terminal's activity. To reconstruct the actual traffic rates of hidden terminals, I utilize training and establish a relationship between the overheard ACKs, the sender's known rate of transmission attempts and the unknown rate of the hidden-terminal traffic.

2.4.3 Identification of Capture Relationships at the Receiver via ACK Rate Analysis

As a final characterization of collision properties, I enable the assessing sender to estimate packet capture relationships at the other, receiving, end of its outbound link. Capture relationships are determined by SNR differences of the sender's and the hidden terminal's packets at the receiver. As such, the differences are time-varying due to channel fading and require timely characterization. However, these differences cannot be directly measured at the sender. PaL's assessment is based on estimation provided by a comparison of the corresponding ACK rates, the ACKs for the sender and the overheard ACKs for the hidden terminal. Capture reconstruction employs the basic causal relationship between the capture effect and throughput: Winning capture reduces IEEE 802.11 backoff, increases the rate of transmissions and results in more received ACKs. Therefore, by measuring the difference of ACK rates for the transmitter and its hidden terminal, PaL estimates the corresponding SNR differences at the receiver. However, this assessment is also prone to sparse characterization of overheard ACKs illustrated in Figure 2.6. I therefore devise a method to interpolate the missing ACK information.

Suppose that the cumulative count of sender's ACKs A_{Tx} is updated at the arrival times t_i, and the count of the overheard hidden terminal's ACKs A_{HT} is updated at the arrival times t_j. To compensate for the difference in updating times and interpolate the missing ACK feedback at the sender, I first divide time in T_B slots. I consider these slots as the reference time intervals for PaL's assessment. To address the slots in which no ACK feedback is overheard, PaL linearly interpolates ACK counters with neighboring slots, thus obtaining continuous ACK representations $\hat{A}_{Tx}(t)$ and $\hat{A}_{HT}(t)$ in T_B time. Finally, the assessing sender estimates SNR differences at the receiver (in T_B time) by comparing the rates of ACK feedback:

$$\frac{d\left(\hat{A}_{Tx}(t) - \hat{A}_{HT}(t)\right)}{dt} \approx \hat{S}_{Tx}(t) - \hat{S}_{HT}(t) \tag{2.1}$$

In Equation (2.1), $\hat{S}_{Tx}(t)$ and $\hat{S}_{HT}(t)$ are the actual SNRs corresponding to the sender's and the hidden terminal's signal levels at the receiver averaged in T_B time intervals. To how timely and effective is this capture reconstruction, I employ correlation index between the ACK-rate indications and the actual SNR differences as a measure of similarity.

2.5 Inbound Link Assessments

Receivers assessing their inbound links have an advantage of being able to directly observe many events that lead to data delivery failures. However, two problems remain: *(i)* receivers may not be able to differentiate between packet losses induced by collisions or channel conditions, and *(ii)* receivers may not be able to attribute packet losses to links at which the losses occur. I will show that both problems are caused by delivery failures that cannot be detected or decoded. Consequently, these two problems affect PaL's key indications. Hence, PaL extrapolates the missing assessment information from undecodable packet losses and readily available measures of successful deliveries and decodable losses (albeit with bit-errors).

2.5.1 Classification of Packet-Loss Causes via Undecodable Packets

Receivers can only identify packet collisions in specific events of packet capture: Specifically, collisions will be identified only when transmission times of colliding packets are decoded and reconstructed to be overlapping. All other collisions, in which only one packet is decoded or both packets are only detected or only one detection is raised, will appear *a priori* similar to channel-induced losses. To address this problem and enable receivers to classify causes of packet delivery failures at their inbound links, I explore losses that are only detected but undecodable. The classification is based on hypothesis that such losses are less likely to occur at links dominated by channel problems than at links dominated by packet collisions. I motivate this hypothesis by properties of wireless receivers, which are designed to effectively address time-varying channel conditions by mechanisms such as automatic gain control or interference cancellation. Consequently, the receivers should initiate packet decoding more frequently in absence of collisions. I evaluate the extent to which undecodable packets are indicative of causes behind packet delivery failures via experiments in controlled settings.

2.5.2 Identification of Transmitter Failure Rates

The second key problem of inbound packet loss characterization is that undecodable delivery failures cannot be attributed to any specific links, i.e., the senders of these links. Therefore, PaL cannot directly estimate the inbound link's actual packet losses. To correct this partial loss perception, I calibrate PaL's receiver-side assessments by offline training. To this end, I extrapolate the knowledge of successful packet deliveries and decodable delivery failures for the measured channel conditions to identify the actual loss rates. The underlying hypothesis is that these parameters combined with the reconstructed knowledge of causes behind packet delivery failures can indicate the actual settings in which the losses occur. Hence, once the setting is identified, the receiver can employ the results of offline calibration and reconstruct its loss properties via calibrated data.

2.6 Implementation and Evaluation Settings

In this section, I describe PaL's implementation and two experimental platforms employed in evaluation: a large setting of wireless nodes consisting of an enterprise IEEE 802.11 network and many experimental platforms in a university department building, and a controlled wireless environment provided by the Azimuth ACE 400 WB channel emulator and nodes employing Atheros wireless cards.

2.6.1 PaL Implementation

I develop PaL on Linux/MadWifi platform[‡], as shown in Figure 2.7. To measure environments in which links operate, I implement a listening interface at I/O tasklets of the MadWifi driver, thus observing all detected and decodable packets before any IEEE 802.11 verification is applied to them. Thus, PaL obtains an insight in a large amount of assessment data from packets that are only detected, unsuccessfully decoded or successfully received. This interface is designed as an individual "virtual" device (MadWifi's VAP) operating in monitoring mode.

To make PaL's data observable, two additional interfaces are created: One shared with kernel-space protocols running on top of any of MadWifi's "virtual" nodes (VAPs), i.e., the 802.11 MAC instances of these VAPs. The interface is provided via a per-assessed-link dynamic data structure visible to all VAPs and kernel code. The other interface exports PaL's data to user-space applications and protocols. The

[‡]The MadWifi Project, http://madwifi-project.org/

exported information can be configured as a stream all PaL's per-packet updates as well as a reporting PaL's assessment results.

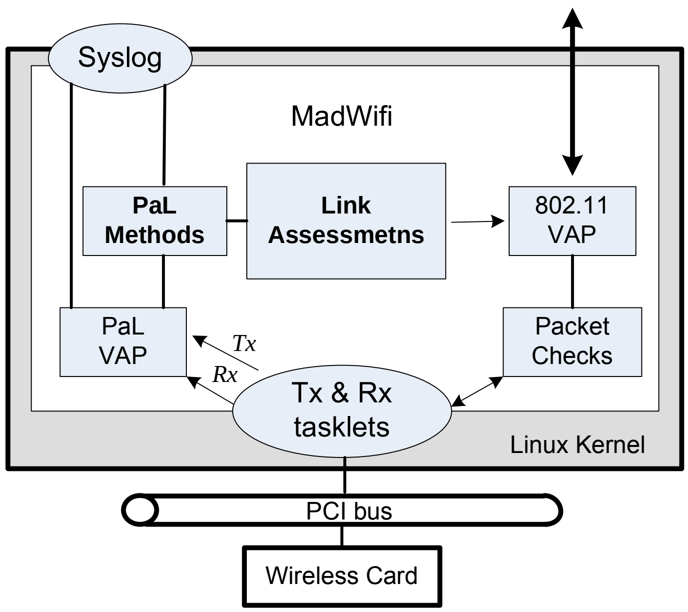


Figure 2.7 : PaL implementation.

Finally, PaL is designed to leverage per-packet information provided by commodity 802.11 devices, as listed in Table 2.1.

2.6.2 Evaluation Platforms

Operational Network. I perform a part of PaL's evaluation in a large indoor setting consisting of an enterprise WLAN network, numerous client computers, smartphones, and several experimental node deployments. In this environment, PaL had no administrative control over any nodes, but the two endpoints of the 25 m link employed in evaluation, as shown in Figure 2.8. The endpoints employed omnidirectional an-

Parameters	Transmission	Reception
Time	no re-Tx	no Rx-Tx
Packet Length	✓	✓
Modulation Rate	✓	✓
Signal (dBm)	Tx power	Rx AGC
Noise (dBm)	no	✓
Retrans. Count	✓	1-bit flag
CRC Check	no	✓
Src./ Dst. Address	✓	✓
Radio Channel	✓	✓

Table 2.1 : PaL's per-packet assessment parameters. (Labels: re-Tx - retransmission; AGC - Automatic Gain Control)

tennas, thus being affected by transmissions of more than 250 identified senders in the links neighborhood. In this operational setting with real users and channel conditions, I analyze PaL's methods for transmitter identification, as well as validate the results of PaL's calibrated methods for link assessment.

Controlled Evaluation Environment. To fully characterize PaL's performance, I extend the evaluation to a controlled laboratory setting. In this setting, I establish assessment calibration and determine how accurate and timely PaL's assessments are. I employ Azimuth channel emulator and nodes with Atheros AR5213 cards. The emulator provides channel conditions that are repeatable in average sense

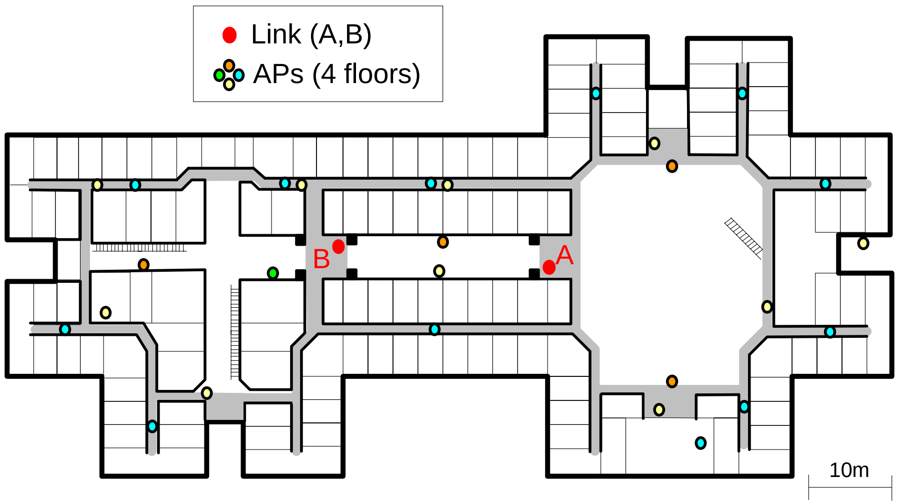


Figure 2.8 : Indoor enterprise wireless setting employed in PaL's evaluation.

for any channel attenuation and fading settings. Moreover, it provides reproduction of reference wireless channels based on ITU recommendations [28]. In the evaluation, I employ the channels representative of static node deployments and deployments up to pedestrian speeds. Being able to configure both channel conditions and communication parameters of all nodes, I train and calibrate PaL in diverse representative environments.

2.7 Evaluation of Transmitter Identification and Profiling

In this section, I evaluate PaL's capability to identify transmitters that affect packet exchange. Evaluation is performed at a link embedded in a large indoor wireless setting illustrated in Figure 2.8. I refer to this setting as operational network.

2.7.1 Assessment Updating Rate

Because a PaL node continuously updates assessments of factors that affect its links, here I analyze the achievable rate of updating in the operational network. Invoking PaL independently at two endpoint nodes of the evaluated link, PaL identified 256 transmitters at one node and 261 transmitters at the other. The aggregate rate of overheard network traffic from which PaL's assessments were updated was 909 $pkts/s$ (of which 546 $pkts/s$ were decodable) at one node, and 819 $pkts/s$ (of which 476 $pkts/s$ were decodable) at the other. Consequently, the updates occurred at about 1 ms intervals without inducing any assessment overhead while being representative of actual communication settings. Moreover, the decodable updates that could be fully characterized (by identifying their senders, packet modulations , SNRs and air-times) were overheard at about 2 ms intervals. For comparison, I observe that such intervals approach transmission times of individual packets. For example, transmission time of a single 1500-byte packet sent at 6 $Mbit/s$ is about 2 ms. Consequently, the alternative approaches based on active and centralized assessments could not provide comparable rates of assessment updating without severely affecting communication performance of the network.

2.7.2 Hamming- and SNR-based Restoration of Transmitter Identities

To assign overheard packets that contain bit-errors to their respective transmitters and links, I employed PaL's methods for restoration of transmitter identities. In reconstruction, PaL identified MAC address corruptions that were up to 20 bits Hamming-distant from the correctly identified transmitters. Employing the Hamming restoration method, PaL uniquely estimated transmitters of about 70% of such packets. Another 20% of "corrupted" addresses had 2 sender candidates which were Hamming-equidistant, while other cases were more ambiguous. The result is illustrated in Figure 2.9.

Focusing only the two-sender candidate cases, I employed PaL's SNR profiling to augment transmitter identification. Figure 2.10 shows distribution of differences between the average profiled SNRs corresponding to the identified sender pairs. Moreover, considering that the average standard deviation of SNR profiles in the network was measured to be 4.3 dB, a decision threshold was set to 5 dB to distinguish between the potential senders. Applying this threshold, PaL estimated sender identities in about 70% of the two-candidate cases. Therefore, Hamming distance criteria and SNR profiling provided a highly effective restoration: In the operational network, PaL uniquely estimated identities of senders for about 83% of decodable delivery failures, thus also identifying the links at which the failures occurred.

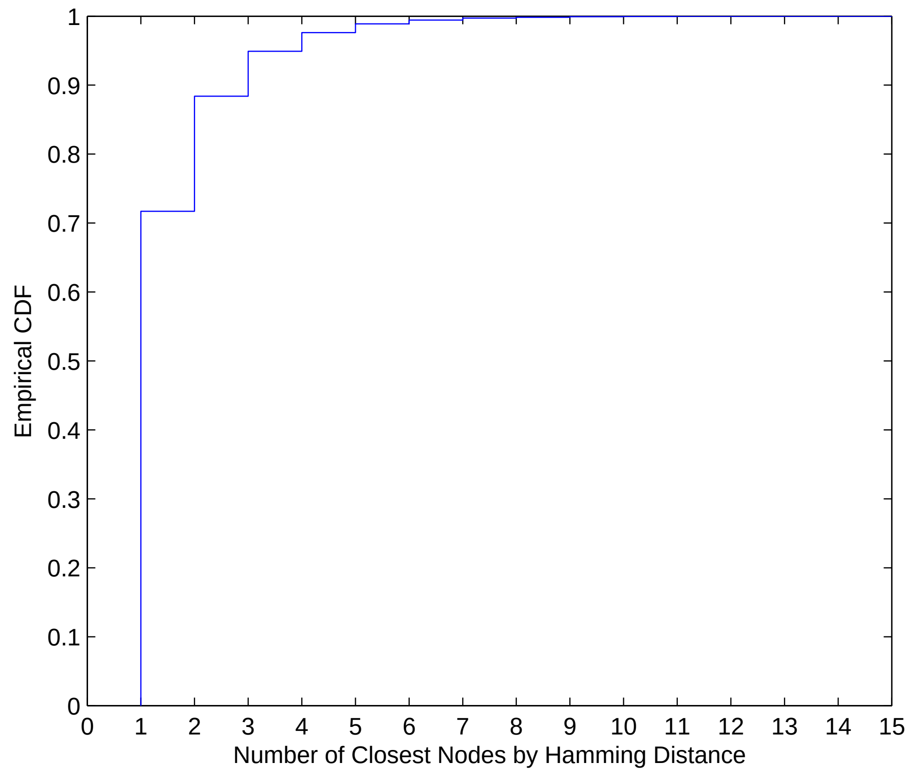


Figure 2.9 : Number of Hamming-closest senders for all cases of per-packet assessment updates that contained bit-errors in MAC address fields.

2.7.3 Identification of Collision Sources via Near Noise-floor Packet Decoding

To identify near noise-floor decoding capabilities of commodity IEEE 802.11 devices, I first evaluated whether the devices can receive packets below the threshold of -85 dBm, i.e., below 10 dB of SNR. IEEE 802.11 standard does not mandate decoding packets in this "near noise-floor" region. However, the experiments in operational network confirmed packet receptions: Specifically, in this region the cards overheard about 5% of all successfully decoded packets, between 20% and 30% of all pack-

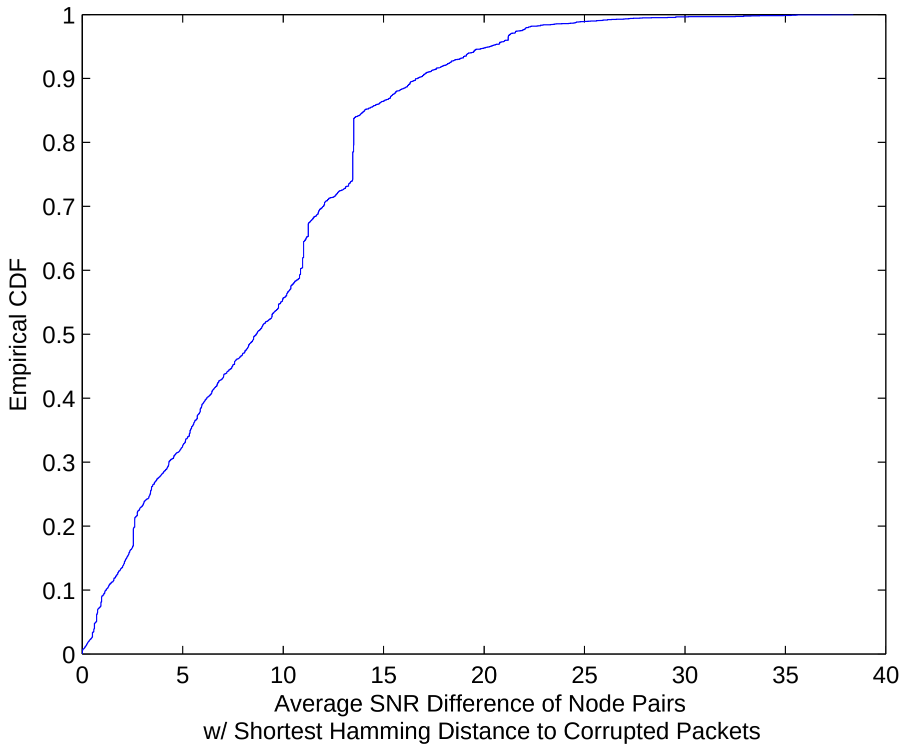


Figure 2.10 : Reconstruction of corrupted sender identities via SNR profiling.

ets containing bit-errors, and about 50% of detected but undecodable packets. In Figure 2.11, I show the results obtained at the link's sender indicating cumulative distributions of the overheard packets based on their decoding and reported SNRs.

Next, I evaluated whether the transmitters of near noise-floor packets that were overheard at the link's sender are the sender's hidden terminals. The principal idea is that the sender would not overhear most such packets and collide with them, thus creating a hidden terminal setting. In the experiment, I established communication between the link's sender and link's receiver and compared the amounts of overheard

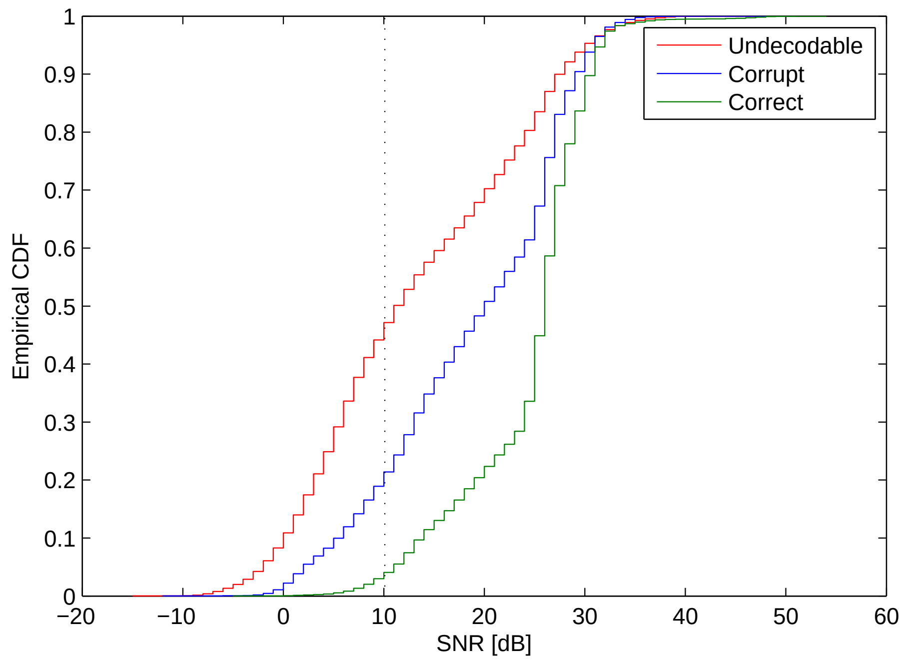


Figure 2.11 : Cumulative distributions of all overheard packets at the link's transmitter based on their SNRs.

packets at each node. Specifically, I focused the transmitters that were overheard at sub 10 dB SNRs at the sender, while being overheard at the receiver at signal levels higher than the IEEE 802.11 sensitivity threshold of -82 dBm. During the experiment, the sender generally overheard an order of magnitude less packets, thus not backing off to most transmissions of its near-noise-flor transmitters. Consequently, the sender and these nodes acted as hidden terminals, thus validating PaL's method for identification of collision sources via near noise-floor decoding. By employing this method, PaL identified 14 and 21 hidden terminals at the two endpoints of the link. Figure 2.12 shows the corresponding results for one of the endpoint nodes.

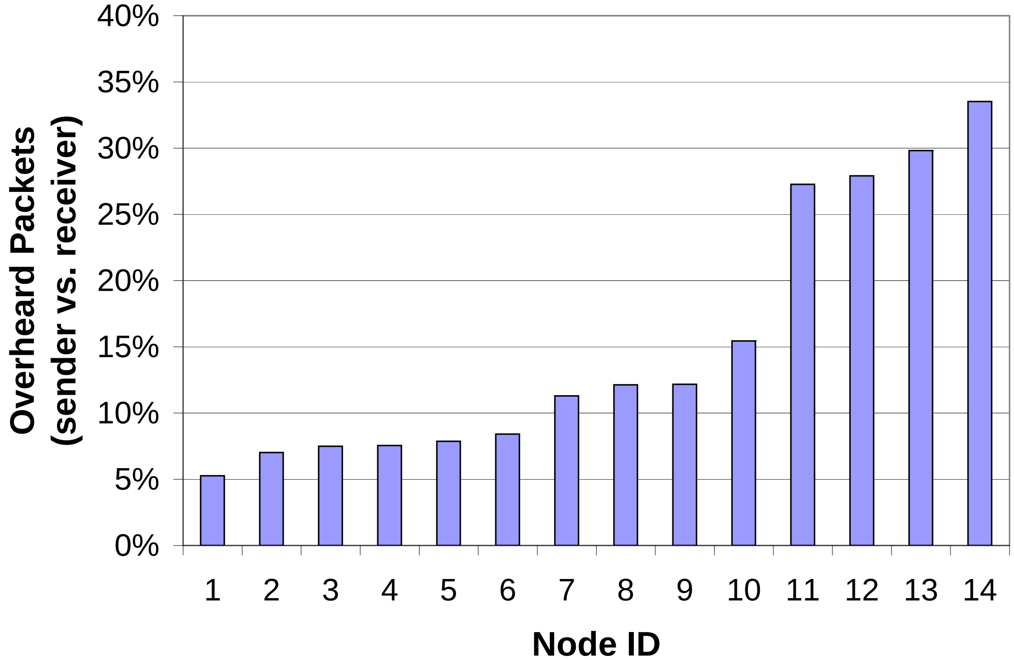


Figure 2.12 : Percentage of packets overheard at the link's sender vs. receiver corresponding to the sender's near-noise-floor transmitters.

2.7.4 Identification of Collision Sources via ACK Feedback

As explained in Section 2.3, each endpoint of the link can identify its hidden terminals by learning about ACK destinations. Results obtained in the operational network revealed that control traffic and presence of access points greatly help this identification method: For example, many client nodes identified themselves by repeatedly evaluating their association options. This enabled PaL to identify additional 5 and 9 hidden transmitters at the link's endpoints.

2.8 Evaluation of PaL's Outbound Link Methods

Here, I evaluate the effectiveness of PaL's methods that inform senders about causes and properties of packet delivery failures at outbound links. Part of the evaluation is conducted in controlled environments to gain a detailed understanding of PaL's performance and to establish off-line calibration for PaL's operation in real networks. To verify these results, I compare them with PaL's assessments obtained in the operational network.

Experimental setting. In the controlled environment, the experiments focus on settings of communication parameters based on 1300-byte payloads transmitted at 6 Mb/s in various topologies. I employ transmission powers that ensure more than 20 dB of reception SNR in absence of fading at the assessed link. Such links carrying actual DATA communications were also found to be predominant in the operational network. Moreover, to evaluate how links perform at different SNRs in fading- and collision-dominated settings, I employ a range of transmission powers in each of the experiments. The presented evaluation is based on multiple 300 seconds tests. In the operational network, evaluation is based on HTTP video streaming provided by VLC software.[§] During the experiments, the link also served an ssh session and exchanged regular control traffic with the rest of the network. Communications over other links were conducted by real users.

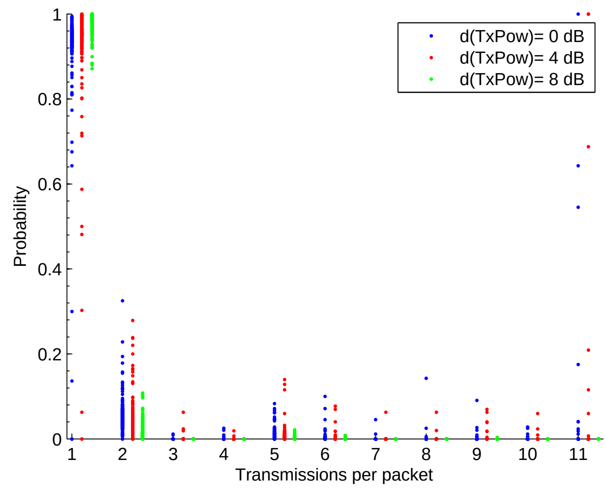
[§]VideoLAN, http://www.videolan.org

2.8.1 Classification of Failure Causes Based on Retransmission Distributions

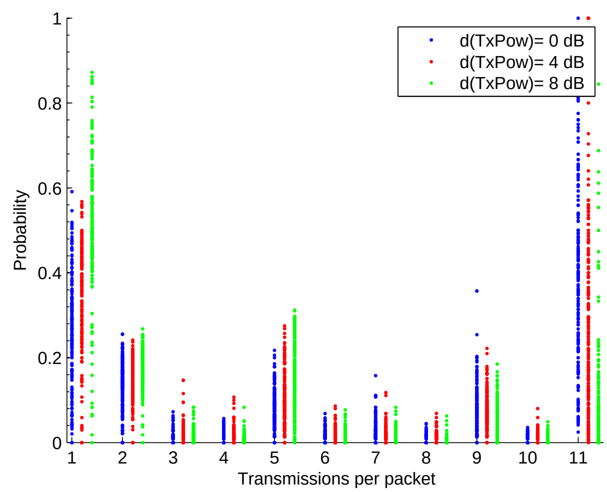
To identify whether channel conditions or packet collisions predominantly cause DATA delivery failures at outbound links, I analyze retransmission distributions. Here, I establish PaL's reference distributions (histograms) and evaluate the extent to which they are representative of collision- vs. fading-dominated environments. The evaluation focuses on two key settings: *(i)* a clique topology in which collisions are rare and losses occur predominantly due to fading per ITU reference channels representative of static deployments [28], and *(ii)* a fully backlogged hidden terminal setting in which collisions are frequent, but losses may also occur due to similar ITU fading channels. A comparison of histograms in these two environments would indicate whether fading and collision environments can be distinguished at outbound links of DATA senders. In each of the tests, PaL continually collects measurements and extracts retransmission histograms in consecutive $T_H = 1$ s intervals.

Figures 2.13(a) and 2.13(b) show the results representing overlayed histogram measurements during the 300 seconds tests. As an evaluation parameter, I chose different transmission powers at the assessing sender and the other transmitter in each tested topology. This enables generalization of findings based on the evaluation of impacts that channel fading has on links with different signal strengths, as well as the impacts of packet capture on links that experience collisions. Our results indicate that in absence of collisions, more than 3 transmission attempts per-packet occurs infrequently (less than 10 %) and channel-induced losses can be effectively addressed by increasing transmission power. On the other hand, in presence of collisions, a greater number of retransmissions is much more frequent, often leading to exhaustion of retransmission attempts. Moreover, increasing transmission power at the assessing sender to a point at which it can capture the receiver from its hidden terminal (at 8 dB difference) is not as effective: Retransmissions from 3 to 10 attempts remain almost unchanged. This is an important result implying that packet capture does not grant successful packet delivery, but instead results in probabilistic delivery outcomes that I characterize by calibration in this thesis. Moreover, consequent retransmissions only increase the backlog of hidden terminals, thus increasing the hidden-terminal collision rates.

To conclude, the nature of packet losses induced by channel effects and collisions is notably different and is reflected in retransmission distributions. Thus, analysis of these distributions provides PaL sender with an effective indication of causes behind packet delivery failures. For example, a 10% threshold set at histogram bins representing more than 3 transmission attempts per-packet would enable PaL to distinguish between collision- and fading-dominated environments. PaL employs such reference threshold to infer actual causes behind packet losses in operational networks. Moreover, *given the significantly less frequent retransmissions in fading-dominated environments, enables us to characterize the two types of losses individually.*



(a) Clique topology with ITU fading channels.



(b) Hidden terminal topology with ITU fading channels.

Figure 2.13 : Reference histograms for fading- and collision-dominated environments.

2.8.2 Identification of Hidden Transmitter Traffic Rates

When PaL identifies that collisions are a dominant cause of failed packet deliveries, it needs to further characterize collisions properties. To this end, PaL first enables the sender to extrapolate information about the traffic rates of hidden transmitters. To establish a mapping between the parameters that the assessing sender can measure and *a priori* unknown hidden terminal activity, I here provide following calibration.

I consider two types of collision-dominated settings according to the amount of information available to an assessing sender: *(i)* the settings in which hidden terminals cannot be identified via their ACK feedback, and *(ii)* the settings in which the assessing sender can partially overhear hidden terminal's ACKs. In the experiments, various contention settings with hidden terminals are reproduced by generating application-layer traffic in intervals from 3 ms to 11 ms per new packet transmission. I refer to such traffic generation as the *offered load*. As a point of comparison, note that the duration of a single packet transmission is about 1.85 ms at the employed 6 Mb/s modulation rate and 1300-byte payload length.

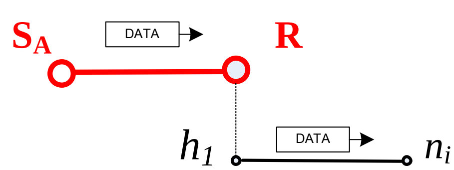


Figure 2.14 : Information asymmetry setting.

Blind Identification. I first establish PaL's calibration in a setting in which hidden terminal activity cannot be overheard, as illustrated in Figure 2.14. Specifically, knowing the sender's percentage of successful packet deliveries and its transmission rate, I identify how this knowledge can be continually extrapolated to identify the activity of hidden transmitters.

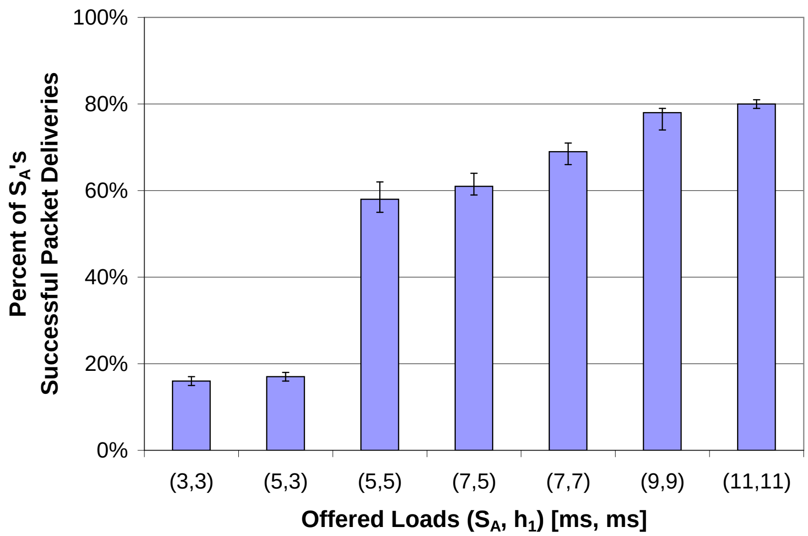


Figure 2.15 : Identification of hidden transmitter's activity in an information asymmetry setting.

In Figure 2.15, I show the results that provide PaL's calibration, plotting the offered loads of the assessing sender S_A and its hidden terminal h_1 on x-axis, and the sender's known percentage of successful packet deliveries at y axis. An example calibration result is that the sender's offered load of 3 ms or 5 ms per packet combined with the measurement of about 18% of successful deliveries indicate that the hidden transmitter h_1 induced the offered load of $3ms$ per packet. Given that such calibration is largely unambiguous up to the 80% of successful packet deliveries where losses become dominated by channel conditions, I confirm that PaL can accurately estimate activity of hidden transmitters by employing only the sender's packet delivery measurements, i.e., being blind to any overheard information.

ACK Analysis of Hidden Terminal Activity. Next, I evaluate the setting in which the assessing sender has more information about the hidden terminal's activity via overhearing ACK feedback, as illustrated in Figure 2.16. PaL employs this information and combines it with the sender's known rate of transmissions in order to extrapolate the activity of hidden terminals.

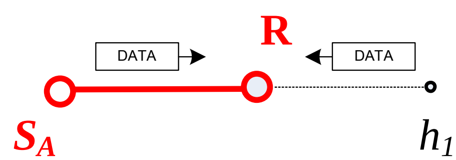


Figure 2.16 : Hidden terminal setting.

In Figure 2.17, I show the results that provide PaL's calibration. An example indication is that the sender's offered load of 5 ms per packet and about 8 pkt/s of overheard ACK feedback sent to the hidden terminal indicate the hidden terminal's offered load of 3 ms per packet. However, in this setting calibration seems to produce ambiguous indications. Specifically, when the offered loads are generated in intervals shorter than 7 ms per packet, the overheard ACK rates provide mostly similar indications. By further analysis, I learned that such indications are correct and representative of actual communication conditions. At these offered loads, collision rates increase retransmission attempts of both transmitters up to a point of full backlog. Therefore, having similar assessment indications for different offered loads does correctly characterize that both transmitters send packets at a full backlog from their cards' firmware (where re-transmission functionality is implemented).

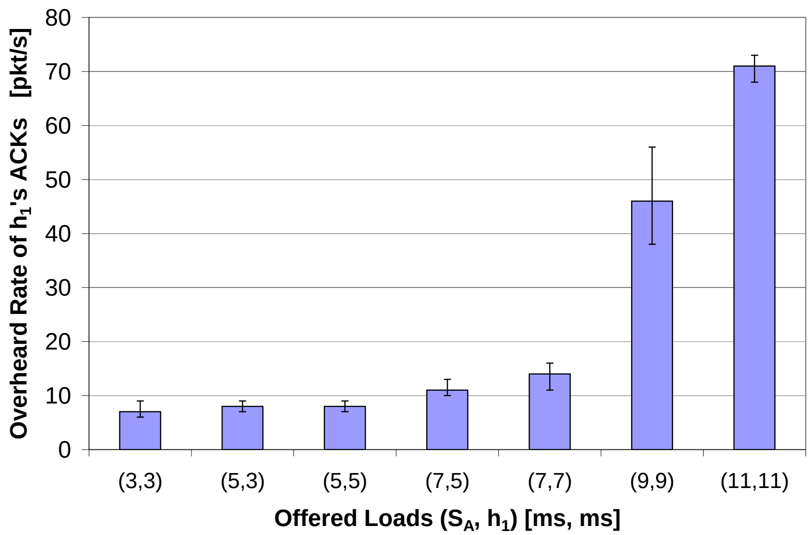


Figure 2.17 : Identification of the hidden transmitter's activity in a hidden terminal setting.

As a final result of this calibration, I make an important remark about hidden terminals, identifying a crucial impact of transmission deafness on operational link settings. Specifically, during the experiments, I identified an increasing transmission deafness of commodity IEEE 802.11 devices occurring at increased the backlogs of retransmissions. Spending most of their time in attempted retransmissions, thus being frequently in transmission deafness mode, both senders overheard only about 10% to 40 % of ACKs sent to their hidden terminals at offered loads generated at 3 ms to 7 ms per packet. Nevertheless, the results in Figure 2.17 indicate that this sparse overhearing of ACKs is proportional to the actual hidden-terminal activity, thus being an indicative measure. Moreover, the results show that changes in hidden-terminal activity can be observed at granularity of just 2 ms of offered load generation.

2.8.3 Identification of Capture Relationships at the Receiver via ACK Rate Analysis

PaL's final task in collision characterization is to enable the assessing sender to identify packet capture relationships at the receiver of its outbound link. To this end, I employ a hidden terminal setting with ITU fading channels and various offered loads at the sender and its hidden terminal, thus emulating different rates of collisions.

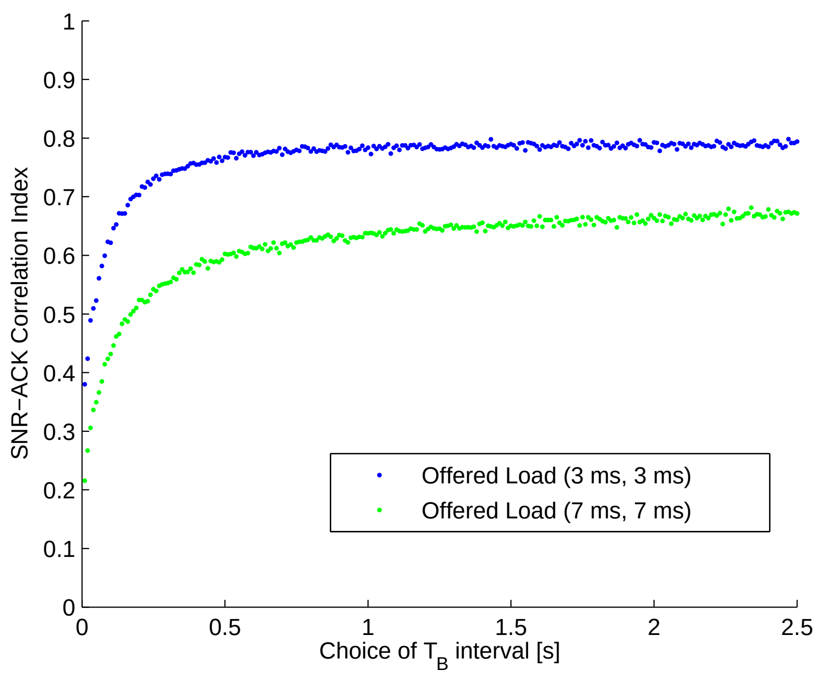


Figure 2.18 : Sender's extrapolation of packet capture relationships at the receiver via the overheard rates of ACK feedback.

Figure 2.18 shows the effectiveness of PaL's sender-side reconstruction of the capture relationships. As a measure of accuracy, I use correlation index between the differences of ACK rates interpolated at the sender in T_b intervals and the actual

SNR differences at the receiver that enable the capture effect. At the receiver, SNRs were averaged over similar T_b intervals. To characterize real-time performance of the proposed method, I evaluated the best choice of T_b intervals in which the ACK feedback is measured and the assessments are produced. These intervals are shown on the x axis.

The results indicate higher correlation, i.e., better reconstruction, for the nearly-fully backlogged hidden terminals generating their offered loads at 3 ms per packet. Specifically, the correlation index reaches the value of 0.8. In this setting packet losses occur dominantly due to collisions that are resolved by capture. Thus, the overheard rate of ACK feedback becomes a representative measure of capture relationships at the receiver. On the other hand, as the offered-load rate decreases (to 7 ms per packet), packets start being lost partially due to channel conditions, thus decreasing the values of the correlation index.

Finally, to identify how timely PaL's assessment can be, I observe the timescales at which the highest accuracy of assessments is achieved. Note a saturation point in correlation index occurring at T_b intervals of about 300 ms. Therefore, *while packet losses can be readily estimated at near-packet-exchange time scales, senders can augment this knowledge further by inferring packet capture relationships at their receivers after 300 ms measurements of link conditions.*

2.8.4 Validation in Operational Network

Here, I apply PaL's sender-side methods to a link embedded in the operational network. I identify dominant causes of packet losses by measuring retransmission distribution of the link's sender during a 45-minute experiment. The resulting histogram is shown in Figure 2.19. According to the results of PaL's off-line calibration previously presented in this section, the shown in-network histogram indicates that packet losses were dominantly caused channel-conditions. I further confirmed this finding by direct measurements at the link's receiver (performed for validation purposes). The measurements confirmed that only about 15% of *decodable* delivery failures were caused by collisions.

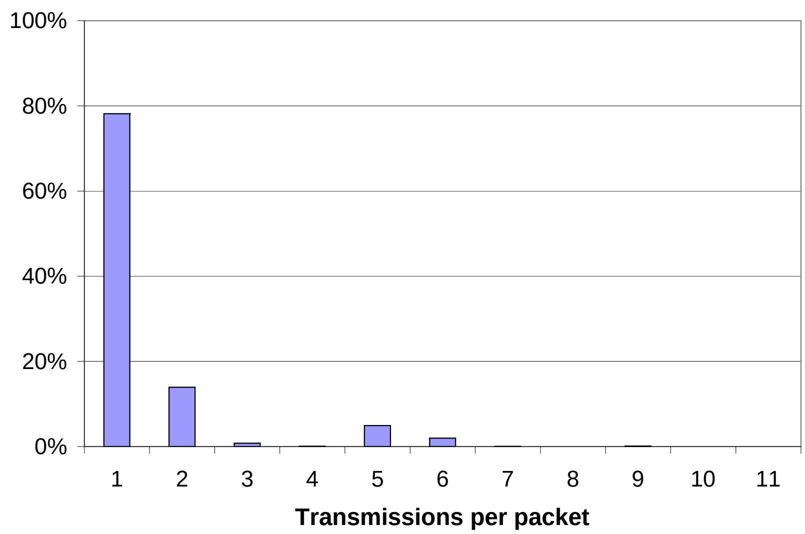


Figure 2.19 : Retransmissions at the assessed link in the operational network.

This result has a key implication on understanding of packet losses in operational networks: *Even though PaL identified tens of hidden terminals, their activity was not* *prohibitively hindering due to: (i) the capability of the link's sender to capture over some of its hidden terminals, (ii) a non-full backlog of nodes in real networks, as well as (iii) due to partially coordinated transmissions of hidden terminals provided by the activity of their shared neighbors. In our network, the activity of hidden terminals was such that only about* 5% *of non-colliding decodable traffic was attributed to hidden terminals by joint analysis at both link's endpoints.*

2.9 Evaluation of PaL's Inbound Link Methods

Here, I evaluate PaL's characterization of DATA delivery failures at inbound links of receiving nodes. While decodable failures are readily addressed by PaL's identification methods (see Section 2.3) and can largely be associated to their links, I here focus on assessment of packet losses that may not be decodable or even detected. Hence, I evaluate PaL's calibration methods that extrapolate the missing information.

Experimental settings. Experimental setup and methodology is similar to the one employed in evaluation of PaL's methods for outbound link assessment (see Section 2.8). Fading-dominated losses are evaluated in a clique topology with ITU channels, while collision-dominated losses are characterized with different activities and transmission powers employed by hidden terminals.

2.9.1 Classification of Packet-Loss Causes via Undecodable Packets

To motivate PaL's receiver-side calibration, I first consider classification of failure causes based only on indications of decodable delivery failures, which fully characterize packet losses and attribute them to their links. Then, to augment PaL's classification, I employ detection of undecodable packets and calibrate PaL for real-time operation.

PaL's evaluation is conducted in two representative packet-loss environments: *(i)* a clique topology with ITU fading channels and seldom collisions, and *(ii)* a fully-backlogged, fading-free hidden terminal topology in which collisions dominate packet delivery failures. Given that detection of colliding packets depends on the existence of packet capture, I evaluate the settings with 0 dB to 8 dB differences in transmission powers at the sending nodes. The 8 dB difference was measured to provide capture effect for the stronger transmitter, thus granting the transmitter at least detection of its packets.

Preliminary Classification without Analysis of Undecodable Packets. Employing direct classification in the clique topology, I confirmed that fading can be correctly identified as a dominant cause of packet losses: In this setting, PaL attributed less than 1% of failed packet deliveries to collisions. However, direct classification of losses in the collision-dominated setting was ambiguous. In Figure 2.20, I present the corresponding results related to different transmission powers at hidden transmitters (indicated on x axis) and measured average rates of collisions at the receiver resulting in identification of both colliding transmitters (shown on y axes). As these results indicate, no collisions were identified for differences in transmission powers less than 4 dB. Thus, PaL cannot identify capture-free collisions as causes of delivery via direct measurements and calibration is needed. Another important result is that PaL decoded numerous packets corrupted in collisions (40 % of all decodable packets were corrupted) but could not identify that corruption was caused by collisions. To this end, I make following conclusions: First, *uncalibrated PaL would inherently overestimate delivery failures caused by channel conditions because many uncharacterized collisions would be attributed to channel losses.* Second, *presented results show that packet decoding does occur in collisions, even when there is no capture effect. This augments PaL's insights and enables us to identify links' modulation* *rates, SNRs and transmission durations for a subset of collision events.*

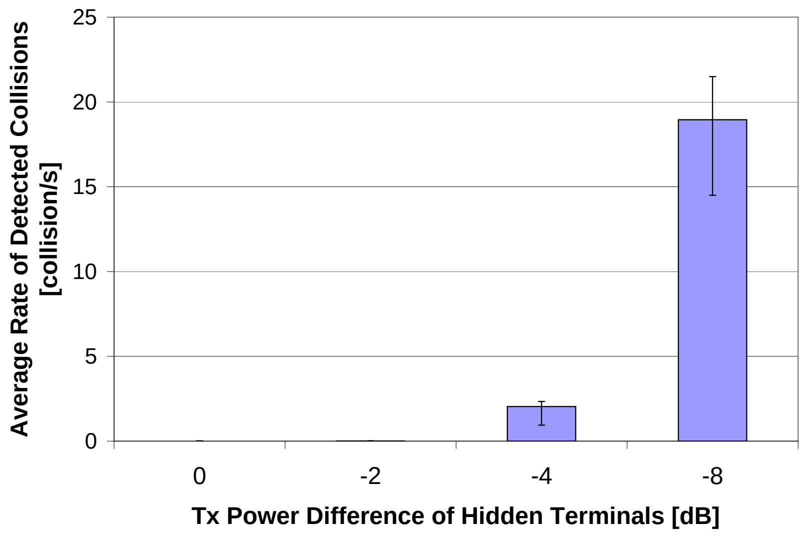


Figure 2.20 : Receiver's direct classification of packet losses caused by collisions.

Classification with Analysis of Undecodable Packets. Next, I augment PaL's classification with undecodable packets identified within the link's SNR profile. While undecodable losses cannot be directly associated to the assessed link, the assumption is that they can indicate loss causes: Wireless receivers should address channel fading better than collisions and produce less undecodable packets in fading-dominated environments. However, in the related research, it is unknown whether this difference in decoding capabilities actually exists and whether it can be effectively employed for link assessment.

In Figure 2.21, I compare the rates of undecodable packet receptions induced by the ITU fading channel in our clique topology and by collisions in our hidden-terminal topology. Both settings were fully backlogged. The results are obtained for various settings of transmission-power differences between the two senders in each topology. As assumed, these results indicate that rates of undecodable packets are more than 10 times higher in the collision-dominated environment. These calibration results enables PaL to distinguishing between the environments with channel- and collision-induced losses in operational settings . Specifically, *a decision threshold set at about* 50 *undecodable failures per second would suffice to make such distinction.*

From these results, I make another important observation about PaL's receiver-side assessments. A large amount of undecodable failures in collision-dominated settings prevents the receiver to fully characterize numerous packet losses. Specifically, the receiver cannot directly identify links at which the failures occurred, thus being optimistic in its assessments of per-link losses. Therefore additional calibration of loss rates is needed.

2.9.2 Identification of Transmitter Failure Rates

PaL's assessments based only on decodable delivery failures are optimistic in estimating packet losses at individual links. Without calibration, such assessments would not be able to attribute the losses that cannot be decoded or detected to their links. Here, I address this problem by establishing PaL's calibration references based on the mapping between actual loss rates (indicated by the link's sender) and measurable rates of decodable delivery failures at the link's receiver. Having identified such mapping, PaL's methods can employ the corresponding results in real-time operation.

Calibration of Loss Rate Indications in Fading-Dominated Settings. I first evaluate

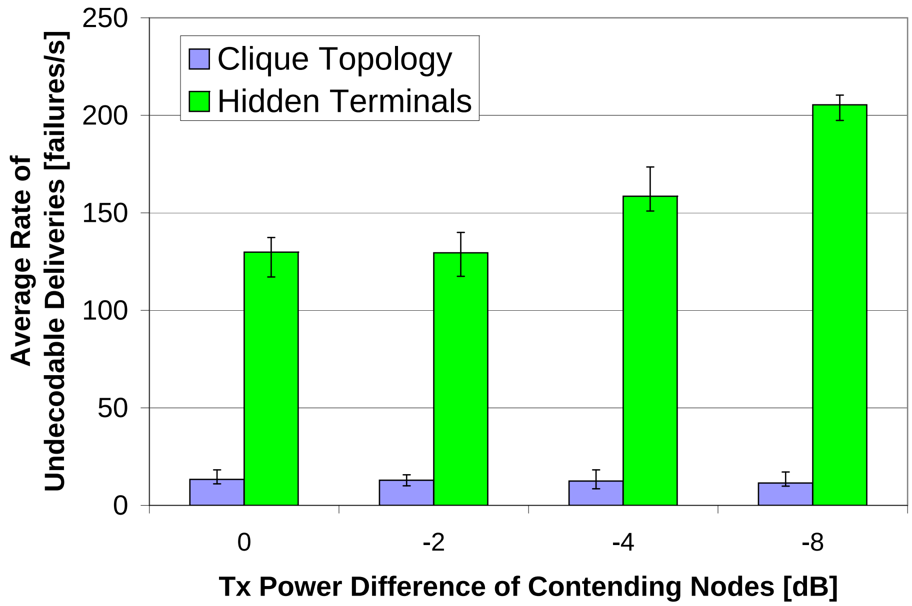


Figure 2.21 : Receiver-side classification of the failure causes enabled by characterization of undecodable packets.

the amount of packet losses that cannot be identified in fading-dominated environments. Then, I try to establish calibration references representative of individual fading settings characterized by various traffic rates and transmission powers.

The results in fading-dominated clique topology indicated that up to 30% of transmissions cannot be successfully received, while the receiver was able to identify that only up to 10% of packets were lost. Therefore, without calibration, only about a third of actual losses can be identified at receivers in conditions corresponding to ITU channels. Trying to establish PaL's calibration references, I could not find any strong relationship between the actual loss rates on one hand and employed traffic rates or transmission powers on the other. Instead, the loss rates were largely random and determined only by the individual channel realizations in each experiment. Nevertheless, empirical bounds of loss rates reported by the sender were established: The bounds were between 12 and 39 packets per second for a wide range of experimental trials.

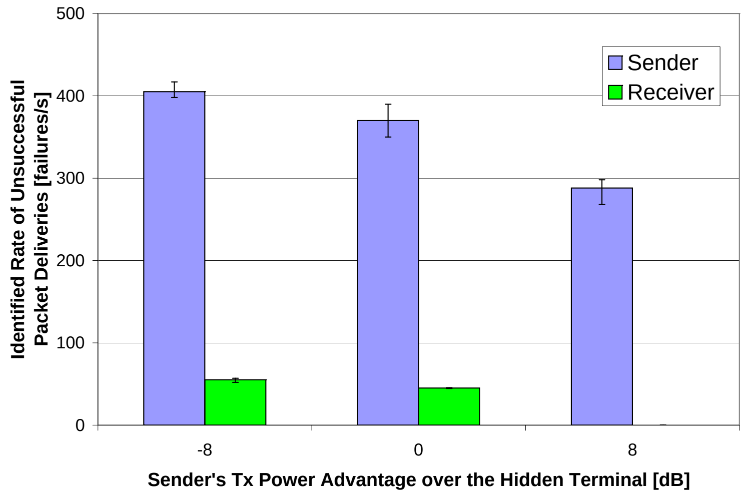
Calibration of Loss Rate Indications in Collision-Dominated Settings. Here, I calibrate PaL's indications in settings with hidden transmitters. I address two types of such settings, one in which packet capture is present and the other in which collisions occur without the capture effect. Results are also provided for different traffic rates of colliding transmitters.

In Figure 2.22(a), I show the results corresponding to settings with different transmissions powers at the link's sender and its fully-backlogged hidden terminal. The results indicate actual loss rates reported by the link's sender and loss rates measured at the assessing link's receiver via decodable delivery failures: Actual loss rates are much higher than identified by the receiver, reaching up to 400 $pkts/s$. Moreover, even when the sender can capture the receiver (at +8 dB difference in transmission powers), loss rate is still significant. This confirms a previous result presented in this thesis, indicating complex and probabilistic nature of the packet capture effect. The results presented here show that in spite of the receiver being able to identify only a subset of actual losses, these measurements are sufficiently different in various settings thus being indicative. Having such indications, PaL employs results shown in Figure 2.22(a) to calibrate receivers' assessments to actual loss rates (also shown in the figure).

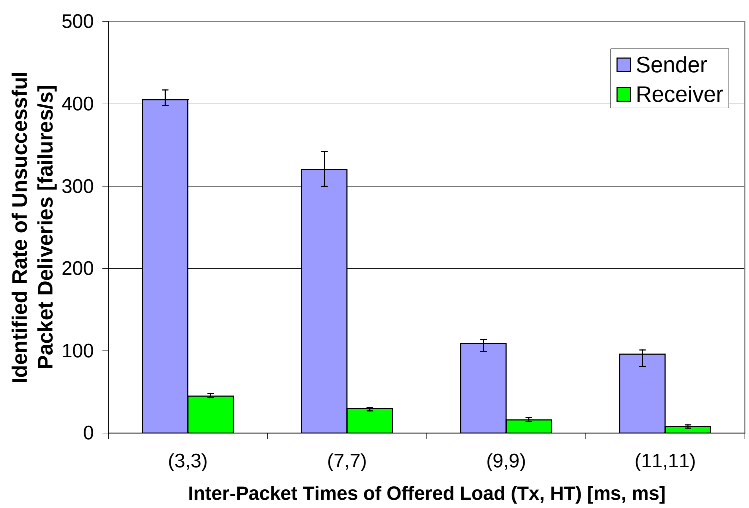
In Figure 2.22(b), I evaluate packet losses occurring due to different traffic rates (offered loads) of hidden terminals. The employed offered loads at the link's sender and its hidden terminal are shown on x axis. Again, the results indicate a significant disparity of receiver- and sender-side loss indications. Also, receiver-side indications uniquely identify each setting, thus enabling PaL to employ the results in Figure 2.22(b) for calibration in operational networks. For example, when a receiver identifies a setting in which colliding senders transmit offered load of $3ms$ per packet, it should calibrate its loss rate assessment of about 40 pkt/s to the actual loss rate of about 400 pkt/s. Moreover, these results indicate that PaL's receiver-side methods can distinguish between the offered-load settings of senders at millisecond granularities of packet generation rate.

Finally, comparing Figures 2.22(a) and 2.22(b) note that loss indications of receiver may be similar in settings characterized by transmission power and traffic rate differences. This raises a question whether the two environments can be distinguished. My experimental results showed that this is the case, the differentiation can be established by receiver's measurements of SNRs and successful packet deliveries corresponding to each hidden terminal.

To conclude: *decodable delivery failures are sufficiently indicative of settings in which delivery failures occur, thus enabling receivers to employ the obtained calibration results for PaL's assessments in real networks.*



(a)



(b)

Figure 2.22 : Reconstruction of senders' activity in settings with: (a) Different transmission powers at hidden terminals, and (b) Various offered loads of hidden terminals.

2.9.3 Validation in Operational Network

Finally, I validate PaL's receiver-side methods via assessments in the operational network illustrated in Figure 2.8. In this setting, I first identify dominant causes of packet losses by measuring the rate of undecodable packet deliveries occurring within the link's SNR profile. PaL receiver identified aggregate rate of undecodable losses to be 21.74 failures per second, which indicates a fading-dominated environment according to PaL's calibration. Correctness of this indication is further supported by direct measurements of collision rates. These measurements indicated only about one collision per second.

Next, I evaluate receiver-side reconstruction of actual loss rates at the assessed link. The receiver identified an aggregate rate of 4.49 decodable failures per second, while the actual loss rate reported by the sender was 14.3 failures per second. Both of these results adhere to PaL's calibration for fading-induced packet losses.

2.10 Summary

In this chapter, I designed, implemented and experimentally evaluated a practical and non-disruptive system for link assessment in statically deployed IEEE 802.11 networks. In contrast to related work, this system enables nodes to independently characterize packet delivery failures at their links without relying on any external assistance in obtaining assessment information. The key contribution is development of methods that extrapolate information about the crucial aspects of packet losses that cannot be directly measured at individual nodes. This work has key implications on network management and diagnostics, as well as a wide range of protocols affected by packet losses.

Chapter 3

Routing Redux: Suppression of Inferior Route Selections

3.1 Introduction

Deployed mesh networks employ routing protocols based on the IEEE 802.11s standard, proprietary protocols such as those developed by Motorola [29], Microtik [30], Cisco [31], and LocustWorld [32], and research routing protocols such as AODV-ST [13] and HOVER [15]. Unfortunately, I will show that common elements of such routing protocols can yield severely inferior routes that persist for long time scales.

In this chapter, I first analyze these common routing elements, referring to them as *node-pair discovery* primitives. These primitives are: (1) constrained flooding, (2) unicast feedback, and (3) temporal ordering of route discovery information. I localize the general problem of *inferior route selection* to one of the inherently incomplete distribution of routing information. Specifically, node-pair discovery primitives can systematically suppress the distribution of information about the best paths for many nodes participating in route discovery. Such *participating* nodes are then forced to re-route to inferior paths based on other received routing information, without even being aware that better paths exist. Consequently, this inconsistent routing state causes nodes to perceive their inferior paths as the optimal ones, thus preventing them from trying to restore their true best paths until a subsequent instance of route discovery.

Second, I develop a *historic ranking principle* targeted towards prevention of inferior route selections and restoration of the true best paths. In particular, this principle provides route selection with valuable information that may otherwise be systematically hidden by the node-pair discovery primitives. To this end, the ranking principle does not induce any additional traffic overhead, but instead relies on historically persistent network properties and readily available routing information from previous route discoveries. Based on this information, I rank all paths previously reported to the node, thus enabling identification of a subset of node's candidate paths that are likely to be the true best path. Therefore, the node infers potentially inferior route selection whenever it fails to receive route discovery reports about this subset of best-ranked paths. Note that this inference also addresses the problem of physically lost routing information, which significantly improves the robustness of least-cost route selection in inherently lossy wireless networks.

Third, I apply the historic ranking principle towards the design of two low-overhead routing primitives that help prevention of inferior route selection and restoration of true best paths. Specifically, while route selection is still based *only* on the presently reported routing information, historically-assisted primitives ensure that no route selection is finalized *until* a node receives route-discovery updates from all of its historically best-ranked paths. The DETER primitive enables a node itself to ensure selection of its best paths, while the RESCUE primitive employs a node's neighbors to initiate recovery from a node's inferior paths by offering it better paths. Recoveries initiated by the DETER primitive have complete information about the node's best-ranked paths, and can therefore make an informed query about the unreported metric costs of specific paths. On the other hand, while the RESCUE primitive does not have such precise ranking information available, it helps address problems that cannot be solved by the DETER primitive, e.g., the losses of the DETER recovery packets, a node's insufficiently trained historical ranking, network re-configurations, etc.

Finally, I preform an experimental and simulation-based evaluation of both currently-employed "node-pair routing" and the proposed historically-assisted routing. I first evaluate the operational behavior of node-pair routing in a large wireless mesh network, Technology For All (TFA) [33]. Evaluation results confirm that current routing primitives indeed fail to consistently select high quality network paths. I also show that poorly selected paths can have significantly higher routing-metric costs, and their duration can extend to minute time scales. Next, I show by measurements that despite a large-scale network having many variable properties (channel state, traffic load, etc.), a number of key properties are largely persistent, e.g., throughputs of isolated paths and throughput rankings of fully backlogged contending links. Having validated these premises of historically-assisted routing, I use simulations to conduct a per-packet evaluation of the deter and rescue primitives. The results show that these primitives largely enable avoidance of inferior route selections. Moreover, when inferior selections do occur, the deter and rescue primitives reduce the duration of such inferior paths by several orders of magnitude, often to sub-second time scales.

The remainder of this chapter is organized as follows. In Section 3.2, I analyze node-pair discovery primitives and show that they inherently cause inferior route selections. In Section 3.3, I introduce the historic ranking principle; while in Section 3.4, I design the DETER and RESCUE primitives. Section 3.5 extensively evaluates routing based on the node-pair discovery primitives, the historically-persistent network properties, and routing assisted by the DETER and RESCUE primitives.

3.2 Origins of Inferior Route Selection

In this section, I show that inferior route selections occur because insufficient routing information is distributed for nodes to identify their least-cost paths. Although packet loss is sufficient to cause this problem, I here focus on a more critical issue showing that node-pair discovery primitives themselves may systematically prevent distribution of the least-cost routing information for many nodes. To this end, I first revisit node-pair discovery primitives and then show how their actions can produce inferior paths.

3.2.1 Overview of Node-pair Discovery Primitives

The main goal of any node-pair route discovery is to identify a single *a priori* unknown least-cost path requested by a *source* node to some specific *destination* node. To this end, the first phase of node-pair route discovery propagates towards the destination accumulating costs of paths to the source, and the second phase propagates back to the source and identifies path cost towards the destination.

Constrained Flooding Primitive. The paths leading to the source node is discovered by constrained flooding. The source initiates flooding of the route discovery packets that accumulate metric costs of candidate paths while traversing each node. Based on reception of such packets, each traversed node identifies potential best-path candidates leading the source and *selects* the least cost candidate for its own path to the source. Each node also *constrains* the flooded discovery by forwarding *only* the discovery packets that report better accumulated path-metric costs. All other discovery packets are silently discarded. Note that when such constrained flooding indeed enables the destination to select its least-cost path to the source.

Unicast Feedback Primitive. The path leading to the destination is discovered by unicasting the discovery-feedback information. Once flooded discovery reaches a node allowed to inform the source about a candidate path leading to the destination*, a node will stop forwarding flooded route discovery packets, select the path leading to the source, and unicast the feedback about its path to the destination in the reverse direction of its just selected path leading to the source. Unicasting such feedback is done under a common assumption that best paths traverse similar nodes in both directions of communication. If this assumption is true, the source would indeed be able to identify its least-cost path to the destination. However, such feedback also forms a *coupling* property of the forward and reverse directions of route discovery that will be crucial in the presented analysis of inferior route selections.

Sequencing Primitive. Routing protocols generally rely on the routing sequence information to temporally order routing packets, constrain flooding of route discovery, and prevent occurrence of routing loops (e.g., see [12]). According to the temporal ordering of routing information, each node has to re-select its path whenever it receives more up-to-date information about an end-point of that path. To this end, the source announces its most up-to-date routing sequence information via the flooded discovery packets, while the feedback packets carry such information about the destination.

*Depending on a configuration of a routing protocol, the discovery feedback can be generated either only by the destination or it can also be generated by other participating nodes on behalf of the destination.

Finally, flooding reduction and loop prevention are provided by discarding the packets that do not carry sufficiently updated routing sequence information to help further route discovery.

3.2.2 Systematic Causes of Inferior Route Selections

I start the analysis of inferior route selections with an observation that routing based on node-pair discovery primitives originates from algorithms that provably identify least-cost paths for *all* nodes in wired networks, e.g., the distributed Bellman-Ford algorithm. However, in order to adapt to wireless environment, "node-pair routing" implements additional overhead reduction techniques that can excessively suppress distribution of routing information, thus forcing inferior route selections. In fact, the only nodes that can generally identify their least-cost paths during the node-pair route discovery are: (1) the source, (2) its requested destination, and (3) the nodes connecting them via the least-cost path. All other participating nodes may *not* be informed about their best paths, while still being informed about their inferior paths which they select based on a premise of more up-to-date routing information. Next, I present analysis of inferior route selections that are systematically caused by such inconsistent routing state.

Cause 1: Partial termination of flooded route discovery by feedback generation. Feedback generation is the core routing primitive that informs the source about its candidate paths to the destination. However, partial termination of flooded route discovery at feedback-generating nodes is sufficient to force *many* nodes

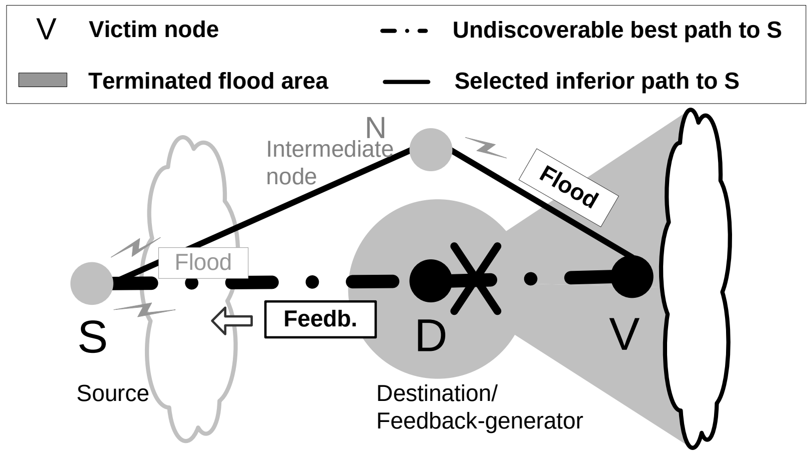


Figure 3.1 : Partial termination of route discovery at the node FG creating a terminated flood area over the victim node V.

to select inferior paths leading to the *source*.

Specifically, such flooding termination partially stops distribution of routing information to nodes deployed in the downstream direction of flooding, i.e., in the *terminated flood areas* shown in Figure 3.1. These nodes then miss being informed about the entire subtrees of paths leading to the source. Route selection problems occur when "hidden" paths are prefixes of best paths to the source for these *victim nodes*. In fact, the victim nodes then select inferior paths due to the unavoidable reception of other flooded routing information. In Figure 3.1, I illustrate an onset of such inferior route selection in which feedback-generating destination D hides the best path leading to the source S from the victim node V. Consequently, node V selects an inferior path whenever it receives any other flooded discovery information, in this example the one sent by node N.

Finally, note that the number of victim nodes can be arbitrarily large, depending on the impact of the terminated flood areas. Also, note that poorly selected paths can have any inferior metric-costs as well as arbitrarily long activity duration, because the best paths of potential victims remain hidden until a subsequent route discovery.

Cause 2: Direction-coupling property of route discovery. Direction-coupling of route discovery is an overhead reduction property that unicasts the discovery feedback *only* over the paths that were previously selected during the flooded route discovery. Such coupling property can suppress sufficient routing information to force *many* nodes to select inferior paths leading to the *destination*. Next, I describe two stages of such inferior selections: (1) initialization by the constrained flooding primitive, and (2) completion by the unicast feedback primitive.

Exclusion of paths leading to the destination initializes inferior route selection during the constrained flooding phase of route discovery. The constrained flooding primitive excludes from route discovery any paths that cannot help the destination to identify a better path to the source. However, this primitive ignores the fact that these "excluded" paths can be best paths of other nodes leading to the destination. Then, due to the coupling property of route discovery, the "excluded" best paths are also not reported in the feedback phase of route discovery and consequently the nodes will never be able to identify them. Note that such exclusion of paths does *not* force any inferior route selection in itself, but it does initiate such selections. Therefore, I refer to the nodes having their best paths excluded as the *potential victim* nodes. In Figure 3.2, I illustrate an initialization phase of an inferior route selection for the potential victim PV whose flooded discovery packet gets discarded at PV's best next-hop FD. Consequently, PV's best path to the destination D, i.e.,

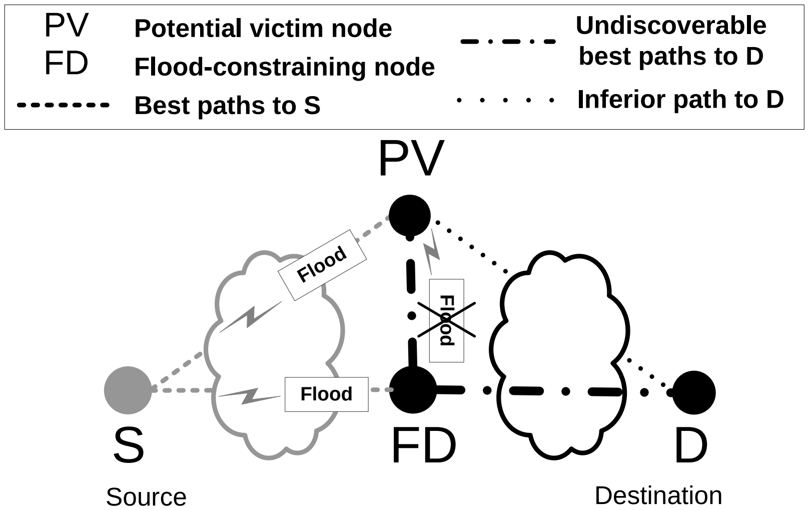


Figure 3.2 : Initialization of a potential inferior route selection of the node PV to the destination D, resulting from the overhead reduction at the node FD.

the path PV-FD-...-D, becomes excluded from further route discovery.

Reception of the discovery feedback over any inferior paths finalizes inferior route selection for the potential victims. Inferior selection occurs whenever a potential victim receives *any* discovery feedback over any of its inferior paths leading to the destination. Ideally, this would never occur if all feedback was forwarded *only* over the true best path of the source-destination node pair, because that path is optimal for all intermediate nodes as well. However, in operational networks this is often not the case: Nodes often have to generate feedback over inferior paths before being informed about the true best path. This occurs because best-path information may be delayed (e.g., due to a longer hop-count distance), lost (e.g., due to packet collisions), or systematically hidden (e.g., due to creation of the terminated flood areas).

While inferior route selection induced by delays and losses occurs in any routing configuration, in Figure 3.3 I illustrate an example of such selection caused by the systematic hiding of paths. In the illustrated scenario, the feedback-generating node FG_1 first *initializes* inferior route selection for the potential victim PV by excluding PV's best path to the destination D, i.e., the path PV-FG_1-D. FG_1 also prevents the node FG_2 from identifying its best path to the source, i.e., the path FG_2-FG_1-S, by covering that path with the terminated flood area (see Cause 1). Second, node FG_2, not knowing now about its own best path to the source, forwards discovery feedback over its inferior path FG_2-PV-S (thus being itself readily mislead to poor route selection). This path coincides with an inferior path for potential victim PV, i.e., the path PV-FG_2-D. Therefore, reception of this feedback *finalizes* inferior route selection also for PV. This demonstrates another important property of inferior route selections: Ones started, these selections spread over victim nodes, leading the nodes to deceive each other into an further poor route selections.

Finally, note that the source is also a potential victim, because it also receives feedback over its inferior paths. However, barring packet losses, the source will be eventually informed about its best path to the destination, because the node-pair discovery primitives do not prevent propagation of best-path information for the source-destination pair. On the other hand, any other potential victims will not generally be informed about their best paths. Inferior route selections for these nodes can have any inferior metric-costs and arbitrarily long durations.

Cause 3: Routing sequence information as a supporting property of inferior route selection. Routing sequence information enables selection of paths based on the most up-to-date routing information. However, the sequencing infor-

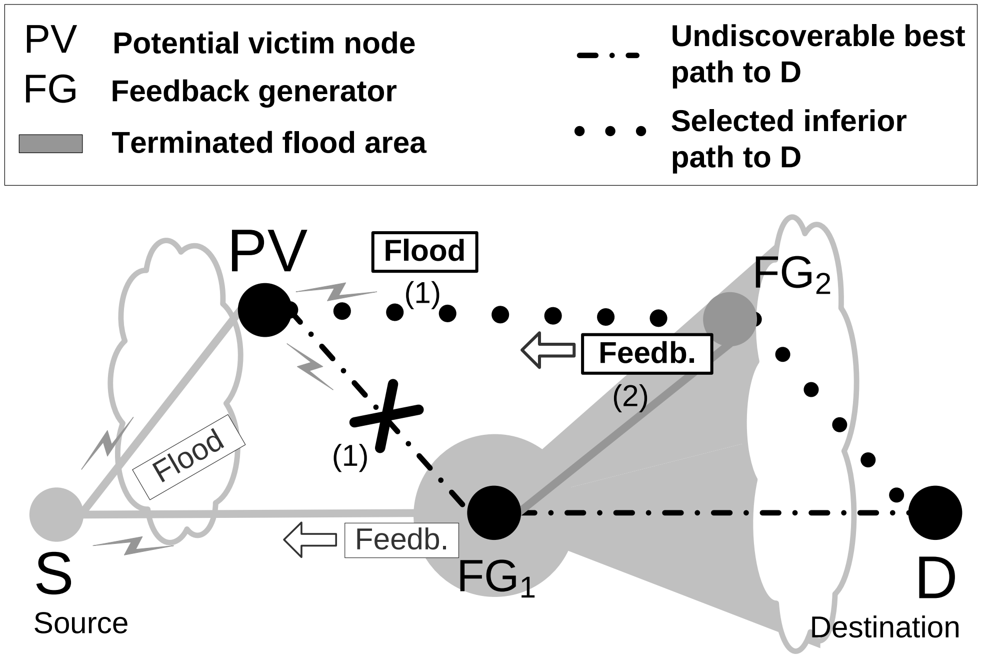


Figure 3.3 : Finalization of inferior route selection of the potential victim PV occurring due to reception of an inferior discovery feedback.

mation is unequally distributed and updated at different nodes in the network, thus enabling the more-recently updated nodes to deceive others to inferior route selections. This occurs in settings in which the feedback can be generated by the nodes participating in a route discovery on behalf of the destination.

Specifically, the way in which the problem occurs is the following: After each route discovery, the destination's most up-to-date sequencing information is reported only to the nodes traversed by the destination's route-discovery feedback. Having this information, these nodes become allowed to generate the feedback on behalf of the destination in a subsequent route discovery. Moreover, these nodes do not have to give up their potentially optimal paths due to the spurious feedback, because their routes are readily up-to-date. On the other hand, being allowed to become feedback generators, the "updated" nodes can induce all previously described problems of inferior route selection for any victim nodes in the network.

Although this work does not address mechanisms that distribute routing sequence information or removes this information from wireless routing, it claims that sequencing information is unnecessary in protocols that employ node-pair routing primitives (e.g., on-demand distance-vector routing protocols). The claim is based on the primary role of sequencing, i.e., the loop prevention functionality provided by monotonically increasing sequence numbers. To this end, I make two observations that suggest obsoleteness of sequencing information: First, each on-demand route discovery, being spread by constrained flooding, is readily sequenced in time, i.e., it already provides the "up-to-date" functionality of sequence numbers. Specifically, each node in the network can identify a new discovery, i.e., the most up-to-date routing information, by the corresponding source and destination addresses of the requested route and the time at which the discovery flooding first swept over the node. Second, loop prevention functionality, provided by the monotonicity of sequence numbers, can be substituted by isotonic routing metrics [34]. The key property of these metrics is that they do not alter monotonicity of path costs as new links (and their costs) are added to the route (and its cost). Therefore, loop prevention would be enabled by the routing metric's monotonicity.

Replacing the sequence numbers with isotonic routing metrics would reduce problems of systematic inferior selections. While this solution requires a careful choice of routing metrics, such metrics are readily dominantly present in wireless routing and include predominantly employed routing metrics: hop-count, ETX and ETT.

Discussion. In the presented analysis, I showed that inferior route selections can systematically occur for any nodes that participate in route discovery, except for the source, the destination, and the nodes connecting them via the least-cost path. Inferior paths can be systematically selected both to the source and to the destination. Therefore, problems of inferior route selection would be significant in any environments in which many nodes share similar end-points of communication, e.g., in the gateway-centric wireless mesh networks. Finally, note that poorly selected paths can have any inferior metric cost and any duration that is only limited by an onset of a subsequent route discovery.

3.3 Historically-assisted Identification of Inferior Route Selection

In the previous section, I showed that inferior route selection results primarily from inherently insufficient distribution of best-routing information. Therefore, to target selection of best paths, extension of route discovery with alternative information sources is needed to compensate for the presently missing information. To this end, the simplest solution would be to continually exchange best-path information for all nodes as is done in the distance-vector and link-state routing protocols. However, such a solution would induce a prohibitively large amount of overhead, thus causing disproportionate reductions of data throughput as shown in [11]. Instead, I develop a historic ranking principle enabling zero-overhead identification of inferior route selections. Historic ranking is a core mechanism of the proposed primitives for preservation of least-cost routing.

3.3.1 Historic Ranking Principle

Next, I define historic routing information, I show how it can be used to identify inferior route selections by the historic ranking principle, and discuss necessary conditions for identification of such selection.

Definition. A node's historic routing information is a collection of paths to each destination and their related metric costs reported during all prior route discoveries in which the node participated.

Maintaining historic routing information enables a node to gain an extensive view of candidate paths that may be hidden during individual route discoveries. Moreover, having an extensive view of candidate paths enables a node to rank the paths according to their previously reported metric costs. Such a *historical ranking* would help identify paths that are likely to become the current least-cost path. Consequently, during route discovery, failure to receive reports from such "likely optimal" paths provides an indication of a potentially inferior route selection.

For this historic ranking principle to correctly identify exposure to inferior route selection, two conditions must be met: (1) historically reported costs of a path must preserve the path's high ranking, i.e., previously best paths must remain feasible candidates for the present best path, and (2) the present best path must have been previously reported to the node.

These conditions are justified for the hop-count path metric merely by the static nature of the network, i.e., the topology is largely unchanging. Moreover, for performance-based path metrics such as [35, 21, 22], the fixed topology should also yield persistence in path performance. For example, if a link suffers from low throughput due to having a long inter-node distance, this condition will not change. Similarly, low throughput can also be caused by persistent contention with a (non-mobile) hidden terminal. Nonetheless, I evaluate and validate these conditions via experiments on an operational wireless mesh network (see Section 3.5).

3.3.2 Implementation of the Historic Ranking Principle

The concept of historically-based path ranking can be applied to any underlying routing algorithm. Here, I propose a ranking implementation for wireless distance-vector protocols such as IEEE 802.11s HWMP [14]. Specifically, to reconstruct best-ranked paths, each node ranks its next hops according to the *end-to-end* path costs reported previously for each destination.

Next, I formally introduce historic ranking principle adapted to the wireless distance-vector routing as illustrated in Figure 3.4.

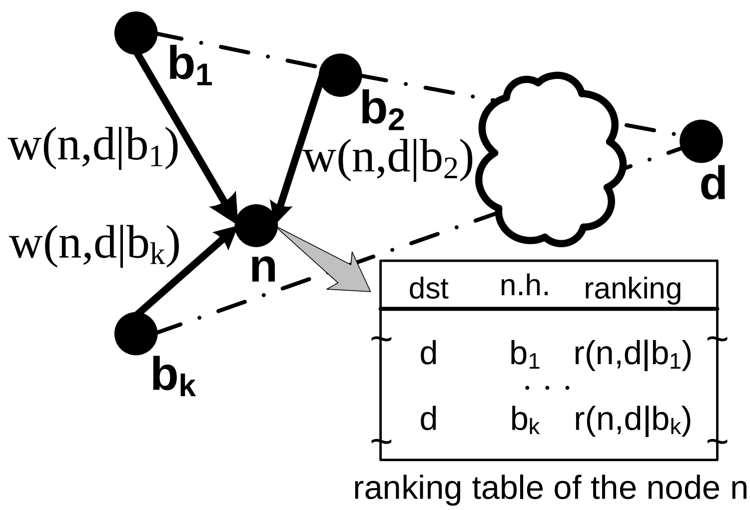


Figure 3.4 : Illustration of the historically-based path ranking that enables a node (node n) to infer which of its neighbors $b_i \in B(n)$ is a potentially best next-hop to a given destination (destination d).

Let $n \in N$ be a routing node, and $B(n)$ be a set of its potential next-hops. Let $w(n, d|b)$ be the path metric cost, i.e., the total cost of on-path links from node n through its next-hop $b \in B(n)$ to the destination $d \in N$. To rank likelihood that the next-hop b can provide the best path to the destination d and to smooth ranking indications, I utilize an Exponentially Weighted Moving Average (EWMA) filter to determine the ranking value $r_i\left(n, d|b\right)$:

$$r_i\left(n, d|b\right) \equiv \left(1-\alpha\right) w_i\left(n, d|b\right) + \alpha r_{i-1}\left(n, d|b\right)$$

$$r_1\left(n, d|b\right) \equiv w_1\left(n, d|b\right)$$

In this definition, $i \geq 2$ represents the total number of route discoveries in which neighbor b reported a path metric cost $w\left(n, d|b\right)$, and α is a configurable coefficient.

By this ranking policy, a neighbor $b_o\left(n, d\right)$ is ranked as a likely *best* next-hop to the destination $d \in N$ if $b_o\left(n, d\right) = \arg\max_{b \in B(n)}\left(r\left(n, d|b\right)\right)$. The ranking of other nodes is performed accordingly. Finally, determining a threshold $T_H(r(n, d))$ that limits the number of next-hops nodes belonging to the highly-ranked set $H(r(n, d)) \supseteq \{b_o\}$ is an implementation decision.

3.4 Deter and Rescue: Historically-assisted Avoidance of Inferior Paths

Having the historically-based assessments of paths that are likely to become the present metric optimal paths, I next introduce two routing primitives: the DETER primitive that enables *prevention* of and *recovery* from inferior paths, and the RESCUE primitive that enables collaborative local *restoration* of best paths.

3.4.1 Historically-assisted DETER Primitive

The DETER primitive is a set of historically-assisted mechanisms a node itself employs during the route discovery in order to ensure selection of its least-cost path. To this end, the primitive addresses two main causes of inferior route selection (see Section 3.2): (1) delayed arrivals of best routing information that induce potentially irrecoverable inferior routes due to the direction-coupling property, and (2) lost or systematically undelivered best routing information that prevents any least-cost routing.

"Wait for the historically-best neighbors" is an informed zero-overhead prevention mechanism that counters delay of best routing information. Relying on the historic ranking, the mechanism *adaptively* delays forwarding of any route-discovery reports until a node receives reports from its best-ranked next-hops for a given destination. Such delayed forwarding not only prevents inferior route selection, but also reduces routing overhead and prevents pollution of a node's historical ranking at its neighbors (which would otherwise occur due it propagating inferior routing information).

During the adaptive delay interval, a node $n \in N$ identifies its presently reported best next hop $b\,(best) = \arg\max_{b_i \in B(n)} \left(w\,(n, d|b_i)\right)$, and verifies that route-discovery reports are received from the best-ranked next-hops $b_k \in H\,(r\,(n, d))$. If all such reports are received, the node infers that it has sufficient information to perform least-cost route selection. The node then selects a path via the *presently* best next-hop b_pb, and advertises a report about that path to the route discovery process. Otherwise, the node waits for such reports until the expiration of a predetermined *threshold* interval $W\,(t)$, and subsequently initiates the inquiry mechanism.

"Historically-best neighbors inquiry" is a historically-informed low-overhead prevention and recovery mechanism that counters undelivered best routing information. Relying on the historic ranking, a node $n \in N$ would employ this mechanism to send a query to a subset of its best-ranked next-hops, asking them for their undelivered route-discovery reports. The node would then potentially re-select its path based on the comparison of its presently best path-metric cost reported by b_pb and the path-metric costs reported via recovery responses. If a better path is received, the node would advertise it to the route discovery process. This ensures that the best path is indeed determined by the *present* best path-metric costs.

3.4.2 Historically-assisted RESCUE Primitive

The RESCUE primitive is a historically-assisted effort of *neighboring* nodes to offer better paths to the node exposed to potentially inferior route selection. The primitive is activated during or immediately after route discovery when all nodes have selected their paths. While ideally RESCUE would be unnecessary, it becomes crucial when a node cannot recover itself to the best path due to effects such as losses of recovery packets or a node's insufficiently trained historical ranking. Next, I describe the RESCUE primitive and address several new challenges arising from its application: (1) each node's general incapacity to know paths of other nodes, (2) potentially significant generation of rescue-related overhead, and (3) potential routing instabilities caused by rescue.

I address incapacity of nodes to know each others selected paths by opportunistically *initiating* the rescue based only on the *local* avoidance of bottleneck links. Accordingly, a neighbor $b_j \in B(s_i)$ (see Figure 3.5) initiates rescue when it infers that it can offer less constrictive link to the node $s_i \in N$, i.e., when $w(b_j, s_i) \leq w(b_j, s_k)$. I experimentally verified this method of recovery initiation in the TFA mesh network [33]. The results indicated that such initiation *does not* prevent better paths from being identified. However, this may produce unnecessary overhead when the total cost of an offered path is higher, i.e., when $w(s_i, d|b_j) \geq w(s_i, d|s_k)$. To constrain such overhead, I limit the number and the interval of rescue retries.

Finally, to prevent routing instabilities that may occur due to fluctuations of present path metric costs during the rescue interval, I employ historic ranking of paths further. Specifically, the node decides to continue processing a rescue offer only when the offer is sent by historically higher ranked next-hop, i.e., if $r(s_i, d|b_j) > r(s_i, d|s_k)$. Note that this decision does not require an offering node to belong to the highly ranked

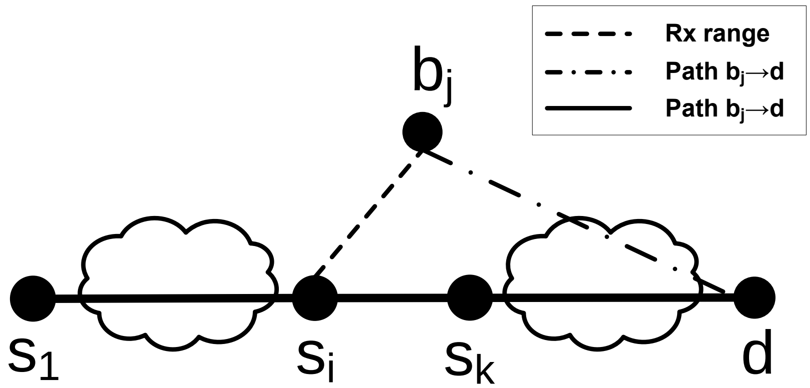


Figure 3.5 : Recovery from inferior path selections. Neighboring node b_j offers re-routing to node s_i upon its inference of path qualities.

set of neighbors $H(r(n, d))$, enabling the RESCUE primitive to overcome limitations of the over-constrained or insufficiently trained highly-ranked sets. Subsequently, the node reselects its current path if the offered path has *presently* lower metric-cost, i.e., if $w(s_i, d|b_j) > w(s_i, d|s_k)$.

3.5 Evaluation

In this section, I employ experiments and measurements on an operational mesh network, as well as simulations to (1) explore the severity of inferior route selection under the node-pair discovery primitives, (2) study the persistence of routing metrics, a key requirement for historically-assisted route selection, and (3) evaluate the ability of the deter and rescue primitives to overcome inferior route selection.

3.5.1 Evaluation Platforms

The TFA network is an operational wireless mesh network that provides Internet access to a residential area of 3 km^2. At the time of measurements, the network consisted of 17 statically deployed backhaul nodes and a single Internet gateway (see Figure 3.6). Each node is equipped with a 15 dBi omnidirectional antenna elevated on a 10 meter pole to provide both the access point functionality and wireless routing. Additionally, a directional link operating over a separate radio channel between nodes 12 and GW serves as a throughput-increasing and interference-avoiding network resource.

TFA replica is a simulation environment that enables a study of routing effects at much finer granularity than possible in TFA itself, providing per-packet observability and perfectly synchronized time references at all nodes. I employ the replica in the ns-2 simulator, which I significantly extend and configure with parameters comprehensively measured in the TFA network. For example, I replicate signal-strength coverage of each node, the range of signal-strength variation of each link, capture

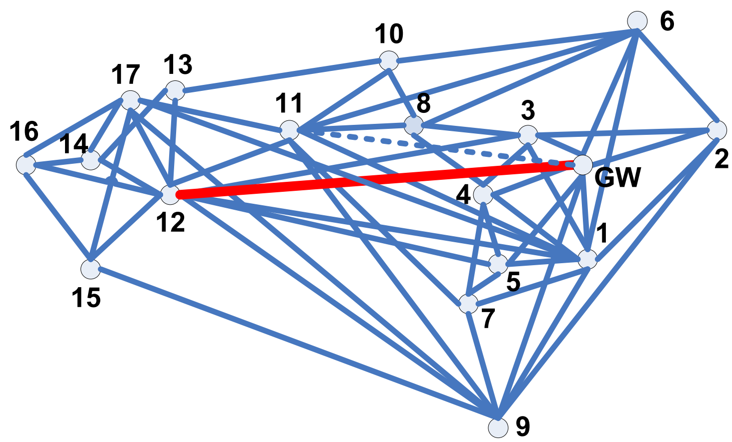


Figure 3.6 : TFA topology and connectivity map.

properties of each pair of links, etc.

Routing protocols. Both in TFA and the replica, I used the routing protocol that employed the node-pair discovery primitives, the SINR threshold of usable link quality, the application-layer gateway announcements, and the distance-vector accumulation of path-metric costs. In the evaluations of historically-assisted routing performed on the TFA replica, this protocol was enhanced with the deter and rescue primitives.

3.5.2 Inferior Route Selections under Node-pair Routing

Here, I measure the main aspects of inferior route selection identified by the presented analysis: (1) the occurrence of inferior paths, (2) the time intervals during which such paths remain selected, and (3) the detrimental effects of inferior route selection on throughput.

Methodology. In the first set of experiments, I choose a representative high-quality path (17-12-GW) and evaluate the ability of "node-pair routing" to correctly select this path. In this evaluation, I employ the hop-count metric that provides a firm reference of path optimality, because the hop-count cost of individual paths is time-invariant, barring link and node outages. To this end, I ensure that the targeted path 17-12-GW was the least-cost path and that it was available during all the experiments. I extract this information from the connectivity records reported by each node's wireless card driver. This first set of experiments is performed during the normal TFA operation with the 5 second measurement granularity during three one-hour intervals, each day for 5 days.

In the second set of experiments, I evaluate the severity of inferior route selection by observing achievable throughputs attained by the "node-pair routing" and by the statically configured best paths (17-12-GW, 16-12-GW, 11-12-GW) that were identified by a large set of preliminary measurements. In this evaluation, I measure throughputs of fully-backlogged TCP flows that contend with the network management traffic of all nodes, and with the traffic of in-home networks outside of my administrative control. The confidence in obtained results is gained by conducting numerous 5-minute measurements over several days.

Results: Occurrence, duration, and impact of inferior paths. Figure 3.7 depicts the hop-count costs and durations of selected paths from the observed node 17 to the GW. The results indicate that only 3 out of 12 selected paths are metric (hop-count) optimal, even though the targeted best path 17-12-GW (denoted as

$2H\_1(Opt)$) was available during all measurements. Moreover, four out of nine non-metric-optimal (i.e., inferior) paths have metric costs that are more than twice that of the available best path. These results confirm analytical findings about the arbitrary costs of inferior paths.

Figure 3.7 also indicates that although the best path $2H\_1(Opt)$ has the longest average duration (max. duration being 27.4 minutes), the duration of inferior paths can be arbitrarily long, i.e., spanning from 5 seconds (the employed measurement granularity) to tens or hundreds of seconds. This result also confirms the presented analytical finding about the potentially long durations of inferior paths limited only by an onset of new route discoveries. Such discoveries occur when the on-path nodes infer that their existing path is broken, or when other nodes initiate route discovery.

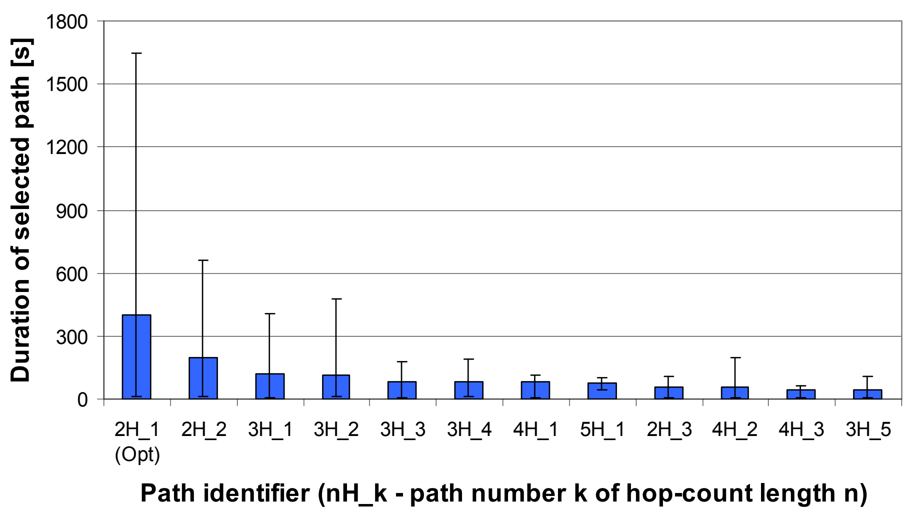


Figure 3.7 : Durations and hop-count lengths of paths selected by the reference node 17. Presented are average, minimal, and maximal durations.

Table 3.1 shows the impact of inferior route selection on the achievable throughputs of nodes. The results indicate that depending on the amount of time a node spends on its inferior paths, poor route selection can reduce achievable throughput significantly, from approximately 20% (node 17) to 80% (node 11). Moreover, note that in the TFA network such inferior paths also negatively impact throughputs of neighboring paths, because the inferior paths fail to include the capacity-injecting link 12-GW and subsequently increase contention with the neighboring paths in the critical gateway area.

Avg Throughput [kb/s]	11 to GW	16 to GW	17 to GW
Node-Pair Route Selection	401.63	847.86	2075.36
Static Best Path	2143.11	1723.02	2570.24

Table 3.1 : Average throughputs attained by the node-pair route selection and by statically set best paths.

Finally, note that the targeted best path 17-12-GW is not only optimal in the hop-count metric, but also in the SINR metric and any throughput-related metric. Therefore, similar inferior route selections would be observed if these other metrics were employed.

3.5.3 Prerequisites for Historically-assisted Routing

Here, I measure the existence of persistent network properties that would enable the historic ranking principle to identify potentially inferior route selections. Of a particular interest are the properties that would support the ranking according to performance-based metrics [35, 21, 22]. Moreover, I evaluate the amount of historic reports about the metric-optimal paths, which is another perquisite for historically-assisted routing.

Persistence of performance-based metrics. To understand whether paths can be ranked according to the performance-based metrics in mesh networks, I evaluate two dominant impacts of the wireless environment on such metrics: (1) the impact of wireless channels, and (2) the impact of contention and interference. I encapsulate evaluation of these two factors in a single type of throughput measurement by employing fully backlogged TCP traffic. The throughput of such traffic is known to be highly sensitive to the both analyzed factors [36].

First, as a baseline, I measure whether persistent throughput ranking can be achieved for isolated paths under the inherently variable conditions of wireless channels. To minimize any contention-related effects on the results, I prevent traffic generation at all TFA nodes that do not belong to the observed path. Second, I experimentally validate persistent ranking of contending wireless links, which are the core elements of path-metric accumulation. In these measurements, I also expose the observed links to additional contention and interference produced by *all* other TFA nodes that generate regular network management traffic (e.g., SNMP, connectivity maintenance, gateway announcements, etc.). The employed sets of measurements consist of numerous 5-minute *iperf* throughput tests conducted during 5 days.

Results. In Figure 3.8, I illustrate how the inherently variable wireless channel impacts the ranking of isolated paths. Specifically, throughput properties of five most frequently selected paths by the node 17 were measured. The results indicate that although the standard deviations of throughputs can be significant (up to approx. 300 kb/s), the average throughput of paths remains sufficiently persistent to enable historical ranking.

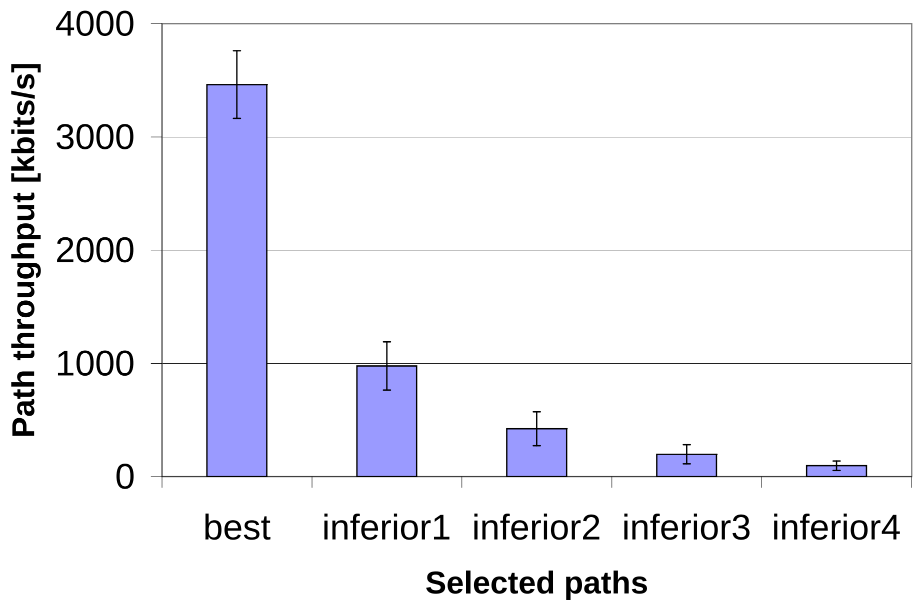


Figure 3.8 : Persistence of throughputs of isolated paths connecting the reference node 17 to the GW. Presented are average values and standard deviations.

Figure 3.9 shows the impact of contention and interference on the historical ranking. Specifically, I measure throughput properties of 4 gateway links in isolation, in contention of all pairs, and in contention of all triplets. Moreover, some of these links act as hidden terminals (e.g., 7-GW and 2-GW; 7-GW and 6-GW), and some can capture over the others (e.g., 1-GW over 7-GW). The obtained results indeed indicate highly variable throughputs within and between contention scenarios. However, the properties supporting the historical ranking still exist. First, in each experimental scenario, average throughput does indicate the ranking of links. Second, using results from all contention scenarios, a node could identify its links that would best contribute to high ranking of paths in varying contention scenarios of real networks. For example, in the presented measurements the two highest-ranked links are persistently 1-GW and 2-GW. Note that since the metric-costs of paths represent accumulation of metric-costs of the on-path links, these measurements indicate that paths can also be successfully ranked under contention and interference.

Finally, note that the network traffic properties would also impact the ranking of paths during regular network operation. Although this may perturb the ranking order of specific paths, the presented results indicate that key ranking components are persistent. Therefore, a subset of highly-ranked paths would exist, which supports application of the historic ranking principle.

Historic reporting and selection rate of metric-optimal paths. The basic condition for historically-assisted ranking to contain the current metric-optimal path is that this path was reported in some previous route discovery, and that the path's reports were sufficiently frequent to update its ranking in diverse network conditions. However, recall from the analysis in Section 3.2 that during any single instance of route discovery, any node may not receive reports about its best path. Therefore, I next evaluate how frequently route discoveries report highly-ranked paths.

To this end, I perform a large number of measurements that evaluate selections of the paths connecting each node to the GW destination. I focus on the reporting of metric-optimal paths, because such paths are likely to be highly-ranked due to the previously described effect of preservation of high ranking. To know which paths were

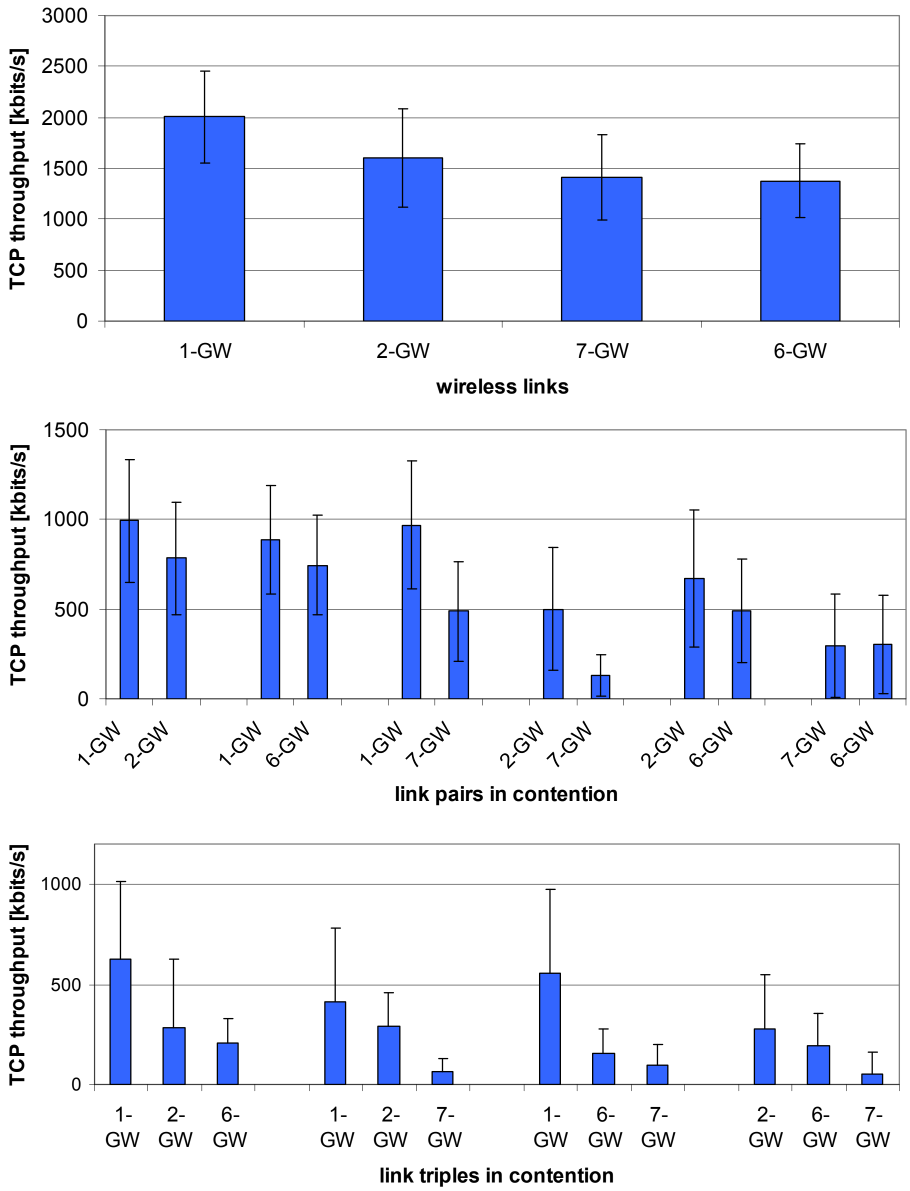


Figure 3.9 : Persistence of throughputs of contending links. Presented are average values and standard deviations.

metric-optimal, I employed hop-count metric in the routing protocol. Moreover, from the preformed measurements, I also extract information about the paths having the highest achievable throughput.

Results. Figure 3.10 presents measurement results obtained during regular network operation for four representative nodes. These results indicate that the neighbors of the GW destination, e.g., node 4, generally preserve their optimal 1-hop paths due to the employed pro-active connectivity maintenance [12]. Next, the nodes having best paths that offer significantly higher achievable throughput than other paths, e.g., nodes 16 and 17, select their metric-optimal paths in more than 50% of measurement samples. Note that node 17 selects its "highest-achievable-throughput" path less frequently, because it has a higher number hop-count optimal paths than node 16. Finally, nodes that are prone to loss-related communication effects, e.g., nodes 10 and 11, may select their hop-count optimal paths frequently, but their throughput-optimal paths are selected in less than 50 % of measurement samples. Nevertheless, given the preservation property of path ranking, the measured rates of metric-optimal path selections are sufficient for a node to identify its path candidates belonging to the highly-ranked path set.

3.5.4 Evaluation of Historically-assisted Routing

Here, I evaluate capability of the deter and rescue primitives to overcome inferior route selection. Specifically, I analyze: (1) metric costs of selected paths, (2) contribution of each primitive towards the restoration of least-cost paths, and (3) the amount of additional overhead related to such restoration.

Evaluation setting. To understand a broad set of factors that are not observable in the operational network, I employ the TFA replica to evaluate the deter and rescue

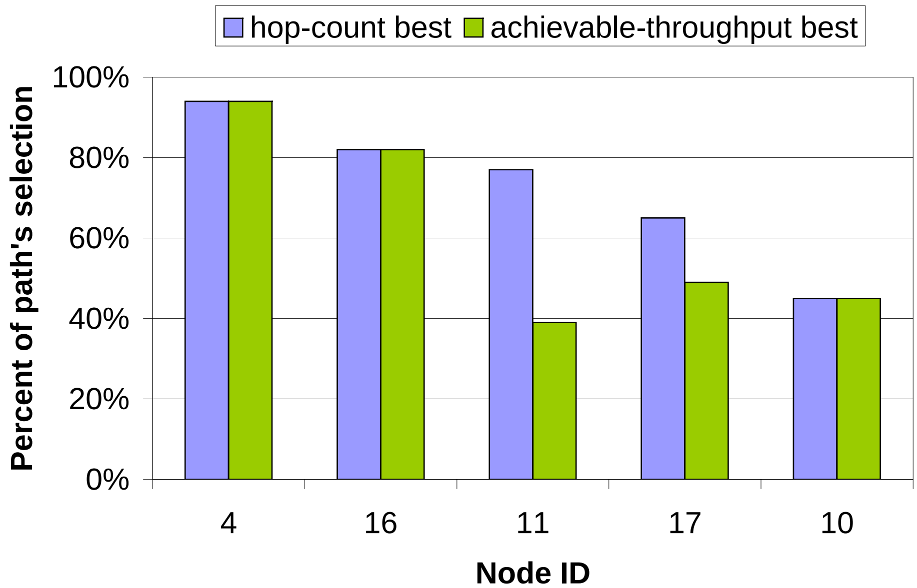


Figure 3.10 : Percentage of metric-optimal route selections of several nodes in TFA network.

primitives. In the preliminary evaluation, I validated that the least-cost paths in the replica are similar to ones in the TFA network, and that inferior paths occur as predicted by analysis.

Next, I configure the historical ranking to only identify a single best path per-destination at each node. I allow the RESCUE primitive to attempt restoration of optimal paths in three equally spaced attempts during the 9 seconds interval following each route discovery. Finally, to enable identification of high-throughout paths, I employ a combination of the ETT metric [21], the SINR metric, and the hop-count metric.[†]

[†]Detailed discussion of how the employed metrics are coordinated to identify high-throughput paths is beyond the scope of this work.

Methodology. I observe route selections of three nodes (11, 16, 17), for which the best paths (11-12-GW, 16-12-GW, 17-12-GW) were identified by preliminary simulations. To invoke route re-discoveries, I gradually increase (in 30 sec intervals) the likelihood of packet loss, which is generally used as a re-routing initiator (e.g., see [12, 37]). In particular, I increase the number of contending nodes in sequence 17→16→11→3→2, in which some nodes act as hidden terminals (11-16, 16-2, 17-2). Similar to the TFA measurements, I employ fully backlogged TCP traffic. Conditions of real networks are emulated by initially randomizing historic rankings of each node by *randomly* starting TCP flows at all TFA nodes in the preliminary phase of each simulation. The results are extracted from 50 experiment runs, each lasting 300 s.

Result: Least-cost property of selected paths. In Table 3.2, I list *all* selected inferior paths and their durations. The results indicate that the historically-assisted routing primitives enable dominant selection of least-cost paths. Specifically, during the thousands of seconds of the simulation time, two observed nodes (nodes 17 and 16) selected only few inferior paths lasting less than a second. The third observed node (node 11), which was always activated during a severe exposure to its readily active and fully backlogged hidden-terminal (node 16), did select a number of inferior paths. However, although this node experienced severe losses of its best-path information, historically-assisted primitives did enable it to restore its best path, often in sub-second intervals. Finally, note that all inferior paths listed in Table 3.2 would be irrecoverable and arbitrarily long-lasting under the node-pair route selection, because they were all caused by undelivered best routing information.

Path	min(T)[s]	max(T)[s]	avg(T)[s]	N	# flows
17 11 0	0.0043	0.0194	0.0102	6	1
17 1 0	0.0106	0.0736	0.0230	5	1
17 1 0	0.0062	0.0127	0.0119	4	2
17 11 0	0.0038	0.0092	0.0073	3	2
16 15 9 0	0.0447	0.0447	0.0447	1	1
16 17 1 0	0.0444	0.0444	0.0444	1	2
11 0	0.0120	65.0204	8.0253	35	1
11 17 12 0	0.0032	7.0011	2.0346	10	1
11 1 0	0.1983	18.7345	9.4664	2	1
11 3 0	0.0165	12.0243	4.2336	4	1
11 0	0.0164	6.0462	2.7022	10	2
11 17 12 0	3.0105	3.0105	3.0105	1	2

Table 3.2 : Duration (T) and number (N) of inferior route selections for a given number of activated on-path TCP flows (#flows).

Result: Individual contribution of the historically-assisted primitives toward suppression of inferior paths. Although the DETER primitive was itself sufficient to prevent any occurrence of inferior paths in many route selections, here, I only analyze suppression of inferior paths that could not be avoided (see Table 3.2). Per-packet analysis revealed that exposure to packet losses significantly impacts the ability of each primitive to suppress inferior paths.

I identified that nodes *not* exposed to a severe impact of loss-related problems generally rely on the DETER primitive to re-route themselves from inferior paths. For example, node 17 relied on this primitive in 12 out of 18 successful best-path recoveries (see Table 3.2). Moreover, for such nodes, I identified that the delay of best-path information causes most inferior route selections. However, the results indicate that all these problems can be resolved within sub-second intervals.

On the other hand, a node exposed to severe packet loss does not generally rely on the DETER primitive, because its requests for recovery are likely to experience collisions. For such node, the neighbor-initiated RESCUE primitive dominantly helps identification of best paths, because the exposure of neighbors to loss-related problems (such as hidden-terminals) is generally different than the one of the node itself. In fact, the RESCUE primitive helped the loss-prone node 11 to recover from 57 of its 62 inferior route selections. In Table 3.3, I provide the timing profile of these 57 recoveries indicating a significant percent of fast (sub-second) restorations of optimal paths.

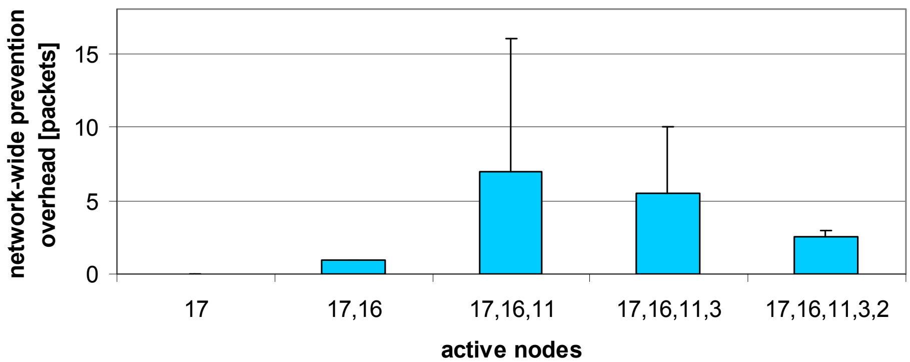
However, inferior paths lasting longer than the 9 seconds rescue interval (see Table 3.3) challenge the ability of the historically-assisted primitives to limit the duration of poorly selected paths. I analyzed each of the 9 selections, discovering that their long duration is caused by the well known effect of TCP traffic outages [36]. These outages prevented the rescue assistance of neighboring nodes because such nodes could not identify poor selection due to the traffic outage on the path. To confirm that the proposed primitives are indeed able to identify inferior route selections, I performed

Recovery interval T	Percent of recovered paths
$T < 1s$	43.9%
$T \in [1s, 3s)$	15.8%
$T \in [3s, 6s)$	14.0%
$T \in [6s, 9s)$	10.5%
$T > 9s$	15.8%

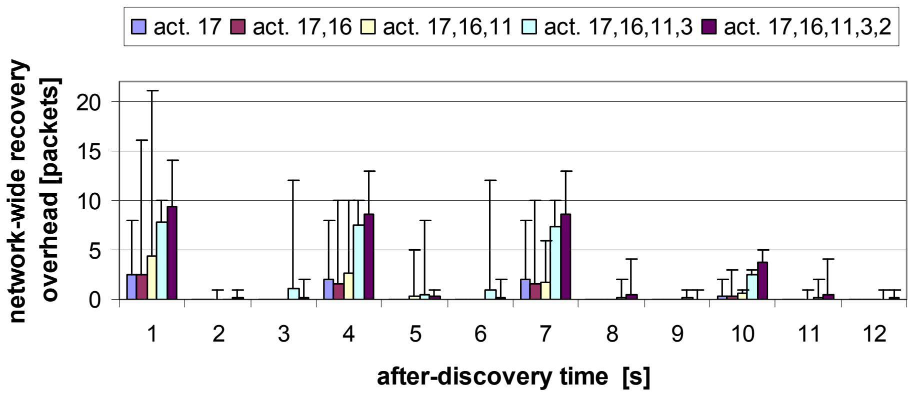
Table 3.3 : Timing-profile of rescues from inferior paths of the node 11, which was exposed to the severe losses of routing information.

additional experiments using 2 TCP flows per node, which reduced the likelihood of on-path traffic outages. In this setting, the presented results (see Table 3.2) confirm that rescue always occurs within the configured 9 seconds rescue interval.

Result: Overhead cost of historically-assisted routing. The results in Figure 3.11 indicate that the total generated network overhead adapts to the increased likelihood of inferior route selection. In particular, the DETER primitive generates most recovery requests when a node is most likely to lose its route discovery packets, e.g., due to an exposure to hidden-terminals (such as the nodes 11 and 16). The average generated overhead is at most 7 pkts for the entire network. The RESCUE primitive also adaptively reduces its overhead as best paths are being recovered. The rescue overhead is somewhat larger because it is employed opportunistically.



(a)



(b)

Figure 3.11 : Total overhead of historically-assisted primitives generated by all nodes: (a) preventive DETER primitive, and (b) recovery RESCUE primitive. Presented are average and maximal values.

3.6 Summary

In this chapter, I showed that widely deployed routing protocols do not distribute sufficient routing information and prohibit many nodes from selecting their least-cost paths. This leads to selection of paths that have inferior metric-costs, but are falsely perceived as the least-cost ones. To address this crucial networking problem, I developed a set of historically-assisted routing primitives that help avoiding such spurious route selections. I showed that historic information can be successfully applied despite the volatile nature of wireless networks. The proposed routing primitives based on this information suppressed selection of inferior paths, generally to sub-second time scales.

Chapter 4

Related Work

4.1 Wireless Link Characterization

Wireless Link Diagnostics. Identification of factors that affect communications over wireless links has generally been addressed by centralized diagnostic algorithms [7, 5, 4, 8, 10, 6, 9]. These approaches employ administrative control over the network and gather network-wide measurement reports to perform link assessments. While these solutions do provide accurate characterization, their assessments are inherently delayed by collection and distribution of assessment information. Moreover, most approaches employ dedicated sniffing devices or additional sniffing cards. A lightweight version of these algorithms was proposed in [38] to use assessment feedback over the link and the knowledge of proprietary PHY-layer details of link's communications. In contrast, PaL enables nodes to individually assess their incoming and outgoing links by employing only local and non-proprietary information exported by all commodity IEEE 802.11 devices. Moreover, PaL does not require any administrative control or exchange of extraneous assessment data. Instead, it enables individual nodes to assess their links in any deployments.

On the other hand, a local assessment methodology that characterizes heterogeneous interference sources is proposed in reference [39]. Commodity 802.11 devices and local information are employed to identify error patterns in decodable packets induced by Bluetooth, WiFi and other sources of interference. In contrast, this thesis addresses a broader set of link problems, including reconstruction of the actual rates and causes of delivery failures at all assessed links, estimation of hidden terminal activities, etc. Moreover, the thesis is the first to show how to employ indications provided by both decodable and undecodable packets in link characterization.

Active Link Measurements. In practice, wireless links are typically assessed via state-of-the-art link metrics [21, 22]. These metrics employ periodic probing sent at a particular packet length and modulation rate to measure link properties. However, actual communications employ diverse sets of packet transmission parameters, thus requiring a large increase in probing in order to produce representative link characterization. In contrast, PaL is non-disruptive and inherently representative of actual parameter settings employed in communications. Moreover, PaL's assessments also provide diagnostic indications of causes and properties of communication problems.

4.2 Wireless Routing

Node-pair discovery primitives. The node-pair route discovery primitives have been employed and studied in both mobile ad hoc networks (MANETs) (e.g., see [18, 17] and the references therein) and static mesh networks (e.g., see [15, 13, 19, 40] and the references therein).

Fortunately, *MANETs* are largely immune to the effects of inferior route selection considered in this work. First, most MANET studies considered random disjoint pairs of mobile sources and destinations in which nodes mostly act as the end-points of route discoveries. As I showed in Section 3.2, it is not the endpoints that are vulnerable to systematically inferior route selections, but rather the participating nodes. Second, if an inferior path is selected regardless, node mobility will limit the lifetime of the route and thus limit the duration and penalty of an inferior route selection. Indeed, MANET routing protocols were shown to correctly identify minimum-hop paths for a high percentage of route selections [18].

In contrast, studies of routing in predominantly static wireless networks have utilized node-pair discovery primitives but focused on link metrics and high throughput routing [13, 15, 14, 40]. However, while new protocols demonstrated throughput gains, no study assessed whether these protocols selected routes that were actually inferior, i.e., whether a better route existed at the time of route selection. Indeed, this work showed that all protocols employing the node-pair discovery primitives will always be systematically prone to inferior route selection irrespective of any individual protocol implementation, or any employed routing metric.

Historic routing information. At one level, all routing protocols employ some use of history and memory in their decisions making, e.g., route caching [16] and time-averaging of routing metrics [35]. In contrast, while route caching utilizes past route selections to reduce overhead by avoiding new route discoveries, the proposed historically-assisted routing primitives jointly consider current routing information and historical ranking of paths. Consequently, the proposed historically-assisted routing enables both selection of presently best paths and identification of potentially inferior paths.

Chapter 5

Conclusion

In conclusion, this thesis addressed local characterization of wireless single- and multi-hop communication resources based on passively collected information. This approach enables nodes to act independently in evaluating complex and time-varying factors that affect their communications. Being non-disruptive to any communications in the network, such characterization is becoming necessary: It makes the wireless medium free from overhead which severely degrades data communications in increasingly growing networks. Two specific topics of this thesis were link assessment and route selection.

In contrast to common approaches to link assessment that require distributed network measurements or link probing, I showed that individual nodes can measure a sufficient number of parameters to reconstruct the key factors affecting packet delivery at their links. Design and evaluation of sender-side methods revealed several new aspects of wireless networking: First, the sender can partially overhear transmissions of its hidden terminals by employing near-noise floor decoding provided by commodity IEEE 802.11 devices. Next, by analyzing re-transmission attempts and sparsely overheard communications of its hidden terminals, the sender can extrapolate causes of its packet delivery failures occurring at the receiver. Similarly, receivers can effectively infer the rates of packet losses which cannot even be detected. The presented link assessment research has numerous implications on other protocols. For example, identifying an increase in traffic rate of hidden terminals, a node may initiate re-routing or adjust its transmission power to counter its packet losses. Moreover, being able to identify activity of numerous nodes in the network, the proposed link-assessment system may be employed to identify malicious network usage.

This work also provided the first systematic analysis of wireless routing primitives, showing that they inherently yield inferior (non least-cost) paths. I showed that selected paths can have arbitrarily high metric-costs and durations, thus severely degrading communications of network users. Moreover, such poor routing affects network operators by selection of paths that do not employ the best available communication resources, thus making such resources futile. To solve this problem, I designed zero-overhead identification of inferior route selections based on historic ranking of paths. My experimental evaluation showed that such identification is feasible due to several persistent properties inherent to wireless networks with static node deployments. Moreover, the developed a set of historically-assisted routing primitives helped suppress route-selection problems or reducing the duration of seldom inferior route selections to sub-second time scales.

Finally, apart from immediate applications, this research opens a new perspective on wireless-protocol design and capabilities of individual wireless nodes. It is my belief that the proposed routing and link assessment approaches can be further improved by advanced techniques for extrapolation and processing of partially observable data. This would lead to further improvements in timescales and detail at which the proposed approaches can provide indications for a wide range of wireless protocols.

Bibliography

[1] J. Moy, "RFC 2328: OSPF version 2," April 1998.

[2] G. Malkin, "RFC 2453: RIP version 2," November 1998.

[3] C. E. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers," in *Proc. of ACM SIGCOMM*, (London, UK), August 1994.

[4] C. R. R. Mahajan, M. Rodrig, D. Wetherall, and J. Zahorjan, "Measurement-based models of delivery and interference in static wireless networks," in *Proc. of ACM SIGCOMM*, (Pisa, Italy), September 2006.

[5] E. Magistretti, O. Gurewitz, and E. Knightly, "Inferring and mitigating a link's hindering transmissions in managed 802.11 wireless networks," in *Proc. of ACM MobiCom*, (Chicago, IL, USA), September 2010.

[6] J. Padhye, S. Agarwal, V. N. Padmanabhan, L. Qiu, A. Rao, and B. Zill, "Estimation of link interference in static multi-hop wireless networks," in *Proc. of ACM IMC*, (Berkeley, CA, USA), October 2005.

[7] A. Kashyap, U. Paul, and S. R. Das, "Reconstructing interference relations in wifi networks," in *Proc. of IEEE SECON*, (Boston, MA, USA), June 2010.

[8] R. Mahajan, M. Rodrig, D. Wetherall, and J. Zahorjan, "Analyzing the mac-level behavior of wireless networks in the wild," in *Proc. of ACM SIGCOMM*, September 2006.

[9] V. Shrivastava, S. Rayanchu, S. Banerjee, and K. Papagiannaki, "Pie in the sky: online passive interference estimation for enterprise wlans," in *Proc. of USENIX NSDI*, March 2011.

[10] D. Nicolescu, "Interference map for 802.11 networks," in *Proc. of ACM IMC*, (San Diego, CA, USA), October 2007.

[11] J. Camp, V. Mancuso, O. Gurewitz, and E. Knightly, "A measurement study of multiplicative overhead effects in wireless networks," in *Proc. of IEEE INFOCOM*, (Phoenix, AZ, USA), April 2008.

[12] C. Perkins, E. Belding-Royer, and S. Das, "RFC 3561: Ad hoc on demand distance vector (AODV) routing," July 2003.

[13] K. Ramachandran, M. Buddhikot, G. Chandranmenon, S. Miller, E. Belding-Royer, and K. Almeroth, "On the design and implementation of infrastructure mesh networks," in *Proc. of IEEE WiMesh*, (Santa Clara, CA, USA), September 2005.

[14] J. Camp and E. Knightly, "The IEEE 802.11s extended service set mesh networking standard," in *Proc. of IEEE Comm. Magazine*, August 2008.

[15] S. Mir, A. A. Pirzada, and M. Portmannz, "Hover: Hybrid on-demand distance vector routing for wireless mesh networks," in *Proc. of ACSC*, (Wollongong, Australia), January 2008.

[16] Y. C. Hu and D. B. Johnson, "Caching strategies in on-demand routing protocols for wireless ad hoc networks," in *Proc. of ACM MobiCom*, (Boston, MA, USA), August 2000.

[17] S. R. Das, C. E. Perkins, E. M. Royer, and M. K. Marina, "Performance comparison of two on-demand routing protocols for ad hoc networks," in *Proc. of IEEE INFOCOM*, (Tel-Aviv, Israel), March 2000.

[18] J. Broch, D. A. Maltz, D. B. Johnson, Y. C. Hu, and J. Jetcheva, "A performance comparison of multi-hop wireless ad hoc network routing protocols," in *Proc. of ACM MobiCom*, (Dallas, TX, USA), October 1998.

[19] K. Ramachandran and I. Sherif and E. Belding-Royer and K. Almeroth, "Routing Stability in Static Wireless Mesh Networks," in *Proc. of ACM PAM 2007*, (Louvain-la-neuve, Belgium), April 2007.

[20] M. Bahr, "Proposed routing for ieee 802.11s wlan mesh networks," in *Proc. of WICON*, 2006.

[21] R. Draves, J. Padhye, and B. Zill, "Routing in multi-radio, multi-hop wireless mesh networks," in *ACM MobiCom*, (Philadelphia, PA, USA), September 2004.

[22] T. Salonidis, M. Garetto, A. Saha, and E. Knightly, “Identifying high throughput paths in 802.11 mesh networks: a model-based approach,” in *Proc. of IEEE ICNP*, (Bejing, China), October 2007.

[23] J. Camp and E. Knightly, “Modulation rate adaptation in urban and vehicular environments: cross-layer implementation and experimental evaluation,” in *Proc. of ACM MobiCom*, (San Francisco, CA, USA), September 2008.

[24] J. Kim, S. Kim, S. Choi, and D. Qiao, “CARA: Collision-aware rate adaptation for IEEE 802.11 WLANs,” in *Proc. of IEEE INFOCOM*, (Barcelona, Spain), April 2006.

[25] S. Wong, S. Lu, H. Yang, and V. Bharghavan, “Robust rate adaptation for 802.11 wireless networks,” in *Proc. of ACM MobiCom*, (San Francisco, USA), September 2006.

[26] P. Husted and W. McFarland, “Method and system for noise floor calibration and receive signal strength detection,” in *Patent 7,245,893*, 2007.

[27] P. Husted, H. Ye, and A. Singla, “Adaptive interference imnunity control,” in *Patent 7,349,503*, 2008.

[28] ITU-R M.1225: Guidelines for Evaluation of Radio Transmission Techologies for IMT2000. Available at: http://www.itu.int/oth/R0A0E00000C/en.

[29] Motorola Incorporates Mesh Spec. Available at: http://www.wi-fiplanet.com/news/article.php/3600221.

[30] MikroTik RouterOS. Available at: http://www.mikrotik.com/.

[31] Cisco Aironet 1500 Series Wireless Mesh AP Version 5.0 Design Guide. Available at: http://www.cisco.com/en/US/docs/wireless/technology/mesh/design/guide/MeshAP.html.

[32] LocustWorld. Available at: http://www.locustworld.com/.

[33] J. Camp, J. Robinson, C. Steger, and E. Knightly, "Measurement driven deployment of a two-tier urban mesh access network," in *Proc. of ACM MobiSys*, (Uppsala, Sweden), June 2006.

[34] J. L. Sobrinho, "An Algebraic Theory of Dynamic Network Routing," *Transactions on Networking*, p. 1160:1163, 2005.

[35] D. S. J. D. Couto, D. Aguayo, J. Bicket, and R. Morris, "A high-throughput path metric for multi-hop wireless routing," in *Proc. of ACM MobiCom*, (San Diego, CA, USA), September 2003.

[36] J. Shi, O. Gurewitz, V. Mancuso, J. Camp, and E. Knightly, "Measurement and modeling of the origins of starvation in congestion controlled mesh networks," in *Proc. of IEEE INFOCOM*, (Phoenix, AZ, USA), April 2008.

[37] D. Johnson, Y. Hu, and D. Maltz, "RFC 4728: The dynamic source routing protocol (DSR) for mobile ad hoc networks for IPv4," February 2007.

[38] S. Rayanchu, A. Mishra, D. Agrawal, S. Saha, and S. Banerjee., "Diagnosing Wireless Packet Losses in 802.11: Separating Collision from Weak Signal,"

[39] K. Lakshminarayanan, S. Seshan, and P. Steenkiste, "Understanding 802.11 performance in heterogeneous environments," in *Proc. of ACM HomeNets*, (Totonto, Canada), August 2011.

[40] A. Subramanian, M. Buddhikot, and S. Miller, "Interference aware routing in multi-radio wireless mesh networks," in *Proc. of IEEE WiMesh*, (Reston, VA, USA), September 2006.